Cyberstresstest

FINANSTILSYNET

FINANSTILSYNET

Indholdsfortegnelse

FINANSTILSYNET

1. Summary

As the first financial supervisory authority in the EU, the Danish Financial Supervisory Authority (the DFSA) has developed and tested a new methodology, cyber stress testing, to investigate and, on this basis, strengthen the financial sector's ability to manage extensive, long-term ICT disruptions. This has been done in collaboration with seven institutions that are critically important for the financial infrastructure. Danmarks Nationalbank, The Central Bank of Denmark, has been an advisory partner. The initiative is inspired by the Bank of England, which is a pioneer in the work of strengthening the operational resilience of the financial sector, among other things by means of cyber stress testing.

What is a cyber stress test?

A cyber stress test is an analytical tool for testing the capacity of firms to manage a severe, but plausible cyber scenario that causes a significant disruption to the firm's ICT services. This means that the test is about the capacity to ensure the continued delivery of critical business services as well as the capacity to recover normal ICT services. This is critical as an ICT disruption could have severe negative impact on the affected institution and its customers. Furthermore, a severe ICT disruption has the potential to affect the financial and operational stability of the financial system.

The test is a desktop exercise which takes place over a longer period of time. The test takes as its analytical starting point that the cyber defenses of the institution have failed. This means that testing the institution's capacity to detect and prevent a cyber-attack is out of scope in a cyber stress test.

The new tool complements institutions' and authorities' other work to strengthen operational resilience, i.e. the ability to respond and recover after a disruption so that critical functions are maintained despite the breakdown.

More than ever, it is necessary to be prepared to manage extensive, long-term ICT disruptions. The dependence on ICT is high and increasing, and so is the threat of disruptions, including from cyber-attacks

The DFSA's first cyber stress test has resulted in valuable learning points for all participating institutions and the DFSA. At the same time, it has strengthened the common understanding of challenges and opportunities in managing extensive ICT disruptions.

Against this background, the DFSA recommends cyber stress testing as a method for investigating and strengthening operational resilience for the financial sector and for authorities and critical institutions in other sectors as well.

The DFSA is currently developing the next cyber stress test in cooperation with Nationalbanken. Whereas the first test focused on the individual institutions' management of an extensive disruption, the aim of the next test is to examine how such a disruption is managed across institutions and at sector level.

2. Indledning

Finanstilsynet har som den første finansielle tilsynsmyndighed i EU udviklet og afprøvet en ny metode, cyberstresstest, til at undersøge og på den baggrund styrke den finansielle sektors evne til at håndtere omfattende, langvarige IT-nedbrud. Det er sket i samarbejde med syv virksomheder, der er kritisk vigtige for den finansielle infrastruktur. Nationalbanken har været sparringspartner.

I en cyberstresstest undersøges organisationers evne til at håndtere cyberangreb og andre omfattende, længerevarende IT-nedbrud, når ulykken er sket. Testen foregår som en desktop-øvelse over en længere periode med udgangspunkt i et konkret, men fiktivt IT-nedbrudsscenarie. Det nye værktøj supplerer virksomheders og myndigheders øvrige arbejde med at styrke operationel robusthed, dvs. evnen til at modstå og genetablere efter nedbrud, så kritiske funktioner opretholdes trods nedbrud.

Cyberstresstest er en undersøgelse af hele virksomheden. For når skærmen går i sort, er opgaven ikke kun at genetablere systemerne så effektivt som muligt. Det handler mindst lige så meget om at sikre, at virksomhedens kritiske funktioner kan videreføres, indtil IT-systemerne virker igen. Hvad end det er kundernes netbank, bankens evne til at udføre betalinger eller handel med værdipapirer, der måtte være ramt. Og sidst, men ikke mindst skal krisen håndteres, så kunderne og andre interessenter ikke mister tilliden til virksomheden.

Det er mere aktuelt end nogensinde at være klar til at håndtere omfattende, længerevarende IT-nedbrud. For afhængigheden af IT er stor og stadig stigende, og truslen om angreb det samme. Aktuelt har Center for Cybersikkerhed (CFCS) opfordret myndigheder og samfundsvigtige virksomheder til at genbesøge og om nødvendigt styrke deres cyberberedskab. Det skyldes, at trusselsniveauet for destruktive cyberangreb mod samfundsvigtig infrastruktur er hævet fra lav til middel.

Finanstilsynet har afsluttet den første cyberstresstest. Testen har givet alle deltagende virksomheder og Finanstilsynet relevante læringspunkter og samtidig styrket den fælles forståelse for udfordringer og muligheder for at håndtere omfattende, længerevarende IT-nedbrud. Derudover har alle deltagerne fået individuelle læringspunkter. Endelig er deltagerne blevet bekræftet i, at test af beredskabet på tværs af forretning og IT er afgørende for at være tilstrækkeligt forberedt det øjeblik, hvor et nedbrud måtte ske.

Finanstilsynet anbefaler på den baggrund cyberstresstest som metode til at undersøge og styrke operationel robusthed både til den finansielle sektor og til myndigheder og samfundsvigtige organisationer i andre sektorer.

Finanstilsynet er aktuelt ved at udvikle næste runde cyberstresstest i samarbejde med Nationalbanken. Hvor den første test havde fokus på de enkelte virksomheders håndtering af et omfattende, længerevarende nedbrud, er formålet med næste runde at undersøge, hvordan et sådant håndteres på tværs af aktører i sektoren, og at kortlægge konsekvenserne af nedbrud på sektorniveau.

Formålet med denne rapport

Det følgende giver en kort introduktion til, hvad en cyberstresstest er, og hvad den kan vise. Fem væsentlige læringstemaer fra den gennemførte test beskrives. De fem temaer giver anledning til spørgsmål, som andre finansielle virksomheder, der ikke har deltaget i testen, og myndigheder og samfundsvigtige virksomheder i andre sektorer kan stille til deres cyberberedskab.

3. Hvorfor cyberstresstest?

Finanssektoren er afhængig af digitale løsninger. Uden IT, ingen bankvirksomhed: Ingen digitale betalinger, ingen aktiehandel, ingen kontooverførsler. Den finansielle infrastruktur er samfundskritisk, og den er bygget på IT.

Trusselsbilledet kræver et solidt cyberberedskab

Den aktuelle udvikling i trusselsbilledet nødvendiggør, at finansielle virksomheder og andre samfundsvigtige organisationer gør, hvad de kan for at være parate til håndtere cyberangreb.

CFCS har udgivet en ny trusselsvurdering i juni 2024, som hæver trusselsniveauet for destruktive cyberangreb fra lav til middel. FE og PET vurderer, at Rusland sandsynligvis er blevet mere risikovillig i forhold til at bruge hybride virkemidler mod europæiske NATO-lande. CFCS vurderer, at denne risikovillighed også omfatter destruktive cyberangreb. Det hævede trusselsniveau gælder Danmark bredt. Hvis Rusland retter destruktive cyberangreb mod Danmark, vil målene sandsynligvis blive udvalgt blandt et bredt udsnit af organisationer i samfundsvigtige sektorer. Derfor opfordrer CFCS myndigheder og samfundsvigtige virksomheder til at genbesøge og om nødvendigt styrke cyberberedskabet.

CFCS definerer destruktive cyberangreb som angreb, hvor den forventede effekt for eksempel kan være personskade, betydelig skade på fysiske objekter eller ødelæggelse af data eller software, så de ikke kan anvendes uden væsentlig genopretning. Det kan for eksempel være såkaldte wiper-angreb, hvor offerets data bliver slettet eller overskrevet.

CFCS vurderer nu, at trusselsniveauet for destruktive cyberangreb er middel. Hertil kommer, at truslen fra cyberkriminalitet mod den danske finanssektor er meget høj. Ifølge CFCS kan cyberkriminalitet potentielt forstyrre tilgængeligheden af den danske finanssektors ydelser. Derudover ser CFCS en udvikling i ransomwareangreb, hvor hackerne ikke kun krypterer data, men også stjæler data fra deres ofre for at afpresse dem yderligere.

Finansielle virksomheder skal være klar til at håndtere mange forskellige typer avancerede angreb – herunder både fra nogen, som har som mål at ødelægge infrastrukturen, og nogen, som har som mål at true sig til eller stjæle penge.

IT-nedbrud kan få store konsekvenser

Et omfattende, længerevarende IT-nedbrud kan få store konsekvenser for en finansiel virksomhed og dens kunder. Men uanset om kun en enkelt virksomhed var ramt fra starten, så ville det også påvirke andre finansielle virksomheder enten direkte eller via afledte effekter. Hvis f.eks. én bank ikke kan gennemføre betalinger, vil andre banker og deres kunder mangle pengene fra disse betalinger i løbet af kort tid. Konsekvenserne af et omfattende, længerevarende nedbrud kan også forværres og spredes, hvis kunder og andre interessenter taber tilliden til den ramte virksomhed. Et sådant tab af tillid har endda også potentiale til at sprede sig til andre virksomheder –uanset om de selv er direkte ramt af nedbruddet.

I værste fald kan finansielle, operationelle eller omdømmemæssige konsekvenser betyde, at det, som starter som et IT-nedbrud, udvikler sig til at få systemiske finansielle konsekvenser.

Den digitale afhængighed, trusselsniveauet og de potentielle konsekvenser af omfattende, længerevarende IT-nedbrud betyder, at der er brug for at styrke den operationelle robusthed. Det skal sikres, at virksomhederne er i stand til at håndtere nedbrud på en måde, så konsekvenserne er håndterbare for borgerne, og samfundet ikke risikerer at gå i stå som følge af et angreb.

Fokus på operationel robusthed

Generelt er der et øget fokus på at styrke operationel robusthed. Bl.a. fokuserer Nationalbanken i Danmark, Det Europæiske Systemiske Risikoråd (ESRB) og Baselkomitéen på risikoen for systemiske implikationer af operationelle nedbrud, og på, hvordan finansielle virksomheders operationelle robusthed kan styrkes.

Konkret anser ESRB cyberstresstest som et vigtigt tiltag for at styrke operationel robusthed. Finanstilsynets arbejde med cyberstresstest er inspireret af arbejdet med lignende test i Bank of England, der har været pionerer på området. Bank of England har siden 2019 gennemført to cyberstresstest og er i gang med en tredje test. I starten af 2024 igangsatte Den Europæiske Centralbanks banktilsyn (SSM) sin første cyberstresstest, der omfatter samtlige 109 finansielle virksomheder under dets tilsyn.

4. Hvad er en cyberstresstest?

En cyberstresstest er et analytisk redskab, der tester en organisations evne til at håndtere et omfattende, længerevarende IT-nedbrudsscenarie, som medfører, at IT-understøttelsen af vigtige forretningsfunktioner fejler helt eller delvist.

Den første cyberstresstest er afviklet som en læringsøvelse for både virksomheder og myndigheder, og metoden er stadig under udvikling.

Ikke test af cyberforsvar, men af evnen til at håndtere et nedbrud

Udgangspunktet for en cyberstresstest er, at virksomhedens cyberforsvar er fejlet. Testen er dermed ikke en test af virksomhedens evne til at forsvare sig, men derimod af dens evne til at håndtere følgerne af et angreb, som vist i **figur 1** herunder.

Figur 1. Hvad testes i en cyberstresstest?

Hvordan udføres en cyberstresstest

En cyberstresstest foregår som en desktop-øvelse, der er bygget op om et fiktivt IT-nedbrudsscenarie. Formålet med testen er at stresse virksomhederne ud over den "normale" hændelseshåndtering, som i forvejen afprøves regelmæssigt både i test og live. Derfor skal det nedbrud, som virksomhederne udsættes for i testen, være omfattende og langvarigt – og noget, som de ikke har prøvet før.

Når testen starter, modtager de deltagende virksomheder nedbrudsscenariet. Uanset virksomhedens cyberforsvar er det i testen ikke muligt at svare, at virksomheden ville afværge angrebet. Nedbruddet er en grundpræmis.

Virksomhederne skal til gengæld svare på, hvordan de håndterer det fiktive scenarie ud fra en række spørgsmål inden for følgende hovedområder:

- Hvordan og i hvilket omfang kan virksomheden videreføre kritiske forretningsfunktioner, som er ramt af nedbruddet?
- Hvordan og hvor hurtigt kan virksomheden genetablere den almindelige IT-understøttelse?
- Hvordan styrer virksomheden sit omdømme under krisen?

Virksomhederne får en længere periode til at redegøre for, hvordan de vil håndtere scenariet. Undersøgelsen foregår altså ikke i realtid, og det er ikke en krisestyringsøvelse. I stedet har virksomhederne mulighed for at gennemtænke håndteringen og at drøfte med tredjepartsleverandører mv.

Virksomhedernes besvarelser analyseres derefter sammen med materiale som f.eks. forretningsnødplaner, IT-genopretningsplaner og planer for kommunikation for at identificere læringspunkter og god praksis individuelt i den enkelte organisation og på tværs af deltagerne.

Finanstilsynets første cyberstresstest

Finanstilsynets første cyberstresstest blev gennemført i 2023. Den havde særligt fokus på detailbetalinger, da det er et samfundskritisk område med umiddelbar betydning for borgernes hverdag. I alt syv virksomheder deltog i testen. Fire SIFI-pengeinstitutter (Danske Bank, Jyske Bank, Nykredit og Sydbank) og tre datacentraler, som leverer IT-ydelser til deltagende pengeinstitutter (JN Data, BEC og Bankdata).

Testen var opdelt i tre faser, hvor virksomhederne skulle indsende besvarelser efter hver fase, som hver varede ca. en måned. Dermed havde virksomhederne tid til at gå i dybden med deres besvarelse. Faseinddelingen blev også brugt til at validere undervejs, at scenariet fungerede efter hensigten, og at der var en fælles forståelse af scenariet.

I den første del af scenariet oplevede bankkunder, at der blev indsat og trukket forkerte beløb fra deres konti. Årsagen hertil var uklar. Opgaven var derfor både at finde årsagen og få fejlen udbedret og samtidig at beslutte, hvordan betalingerne og kommunikationen til kunder m.fl. skulle håndteres, mens der var usikkerhed om, hvad der foregik. Anden del af scenariet var et såkaldt supply chain-angreb. Her var en tredjepartsleverandør af kritisk IT-understøttelse ramt. I scenariet valgte Finanstilsynet, at det skulle tage leverandøren ca. en uge at udvikle en løsning, som gjorde, at systemerne virkede igen. Det betød, at nøglefunktioner i det ramte pengeinstitut var ude af drift i minimum syv dage, uden at virksomhederne havde mulighed for selv at genoprette systemerne.

Der er mange, forskellige scenarier, der er relevante at teste. Valget faldt på ovenstående til den første test, fordi det omfattede både forskellige kritiske forretningsfunktioner, forskellige typer af nedbrud og en længere varighed.

En del af virksomhederne valgte at simulere en virkelig krise ved at gennemspille en lang række møder i virksomhedernes forskellige interne og eksterne beredskabsfora for på den måde at diskutere sig frem til, hvordan virksomhederne ville agere på angrebet. Derefter beskrev virksomhederne i test-besvarelserne deres analyser af situationen, og hvilke handlinger de ville sætte i værk med udgangspunkt i deres eksisterende beredskabsplaner og øvrige setup. På den måde er cyberstresstesten en krævende, men samtidig også meget praktisk orienteret testform.

Det er Finanstilsynet, der har iværksat testen, men den er i vid udstrækning udviklet i samarbejde med de deltagende virksomheder og med sparring fra Nationalbanken. F.eks. er angrebsscenariet udarbejdet med input fra deltagerne for at sikre, at scenariet var relevant for dem. Undervejs i test-forløbet fik deltagerne også mulighed for at give feedback og stille spørgsmål, så testen kunne justeres undervejs. Finanstilsynet har haft et meget godt samarbejde med de deltagende virksomheder, der har bidraget konstruktivt til at få mest mulig læring ud af testen.

5. Hvad afdækker en cyberstresstest?

De væsentligste læringstemaer fra Finanstilsynets første cyberstresstest er beskrevet nedenfor i form af:

- generelle spørgsmål, som kan bruges til at afdække organisationers evne til at håndtere omfattende, længerevarende IT-nedbrud
- konkrete læringspunkter fra Finanstilsynets første cyberstresstest.

---

1. Hvor længe vil det tage at genetablere normal IT-understøttelse?

I en cyberstresstest er et af hovedspørgsmålene, hvor længe det vil tage at genetablere den normale IT-understøttelse i det konkrete nedbrudsscenarie. Det er vigtig viden, for nedbruddets længde er afgørende for den øvrige indsats – i hvilken grad er der brug for nødplaner eller endda alternativ IT-understøttelse? Hvilken kommunikationsindsats er der behov for? Og hvad med kundeservice?

Trusselsbilledet betyder, at det er nødvendigt at forberede sig på længerevarende IT-nedbrud og nye typer af nedbrud. Hvis man f.eks. er ramt som følge af angreb på en tredjepartsleverandør, kan man risikere at være afhængig af den ramte leverandør for at kunne genetablere egne systemer. Hvis man er ramt af omfattende ransomware, er genetablering en kompliceret og langvarig proces, hvor man bl.a. skal sikre sig, at angriberne er fjernet fra data og systemerne, før man overhovedet kan gå i gang. Virksomheder, som er blevet ramt i virkelige angreb, har oplevet, at det har taget uger at genoprette IT-driften – og endda længere. Og i lyset af udviklingen i trusselsbilledet er nedbrud, som ikke er set før, også plausible.

Læring fra første cyberstresstest: Genetablering kan tage lang tid

Den anden del af nedbrudsscenariet i cyberstresstesten var designet, så virksomhederne bl.a. blev ramt af et omfattende nedbrud, som strakte sig over ca. en uge. Dvs. at varigheden af IT-nedbruddet blev pålagt virksomhederne i testen. Det var ikke muligt for virksomhederne selv at genetablere den almindelige IT-understøttelse, fordi nedbruddet skyldtes et sikkerhedsbrud hos en tredjepartsleverandør.

Læringen af det er for det første, at virksomhederne ikke altid selv til fulde er herre over, hvor lang tid genetablering tager. Virksomhederne kan bl.a. være afhængige af kritiske komponenter fra tredjepartsleverandører for at opretholde vigtig forretningsdrift. Det er vigtigt at have afdækket sådanne afhængigheder på forhånd. Og at have analyseret, hvilke hovedtyper af nedbrudsscenarier virksomheden kunne blive ramt af, og hvor længe genetablering forventes at tage i sådanne. Det er en forudsætning for at tage tiltag til at

forkorte reetableringstiden, hvis den viser sig at være for lang. Det er også en forudsætning for at sikre, at forberedelsen af nødplaner, krisekommunikation mv. er kalibreret til den forventede nedbrudslængde, også af ekstreme, men plausible scenarier.

For det andet viste testen, at selve genetableringen – trods eksterne afhængigheder i nogle tilfælde – kan planlægges på forhånd for at sikre, at genetableringstiden bliver så kort som mulig. Her er det væsentligt at sikre, at der er planer for alle relevante hovedtyper af nedbrudsscenarier, da der er stor forskel på, hvad der skal til for at genetablere i forskellige scenarietyper. I tilfælde af f.eks. brand i et datacenter vil genetablering typisk kunne ske i et andet, spejlet datacenter. Men i tilfælde af f.eks. ransomware, hvor data krypteres, vil det ikke være muligt at skifte over til et andet datacenter med spejlede data – for disse vil i så fald også være krypteret. Her vil der være brug for andre tiltag.

---

2. Hvordan kan kritiske forretningsfunktioner videreføres uden normal IT?

En cyberstresstest belyser også, om virksomheden har tilstrækkelige forretningsnødplaner, der kan bruges til at opretholde kritiske forretningsfunktioner. Ved virksomheden f.eks., hvilke betalinger der er kritiske, og hvornår de forfalder? Er der planer for, hvordan betalinger foretages, når den normale IT er ude af drift? Og hvor længe det er muligt at fortsætte med at bruge nødplanerne? Har planerne vist sig anvendelige og tilstrækkelige i tests?

Cyberstresstest kan også give anledning til overvejelser om, hvorvidt virksomhederne kan styrke deres **IT Service Continuity**, dvs. om de i tillæg til manuelle nødplaner på forhånd kunne undersøge, om der findes alternativ minimums-IT-understøttelse, eller om noget sådant eventuelt kunne udvikles på kort tid. På den måde kan testen medvirke til at identificere, om nødplanlægningen kan og bør optimeres.

Læring fra første cyberstresstest: Forberedelse er afgørende

Det stod klart under det længerevarende IT-nedbrud i cyberstresstesten, at det er afgørende, at de forretningsnødplaner, virksomhederne har, modsvarer den tid, som virksomheden forventer, at det vil tage at genetablere den normale IT-understøttelse efter et ekstremt, men plausibelt nedbrudsscenarie. De skal også modsvare de hovedtyper af nedbrud, der er identificeret. Eksempelvis vil det typisk være relevant, at nødplaner dækker, hvis IT-systemer ikke virker. De skal også dække, hvis nedbruddet består i, at centrale oplysninger i systemerne er forkerte, f.eks. fordi de er manipuleret, eller hvis fortrolige oplysninger er blevet lækket.

Testen viste også, at det er vigtigt, at planerne er testet og anvendelige i praksis. F.eks. er det afgørende, at man har sikret sig, at man under et nedbrud faktisk ville have adgang til kritisk data, som anvendes i en nødplan. Og i en tilstrækkeligt opdateret form.

Endelig viste testen, at det er vigtigt, at virksomhederne har klarlagt på forhånd, hvilke funktioner der er kritiske for både virksomheden selv og for dens kunder, hvilke funktioner man har kapacitet til at håndtere i forskellige nedbrudsscenarier, og hvor længe.

I en ekstremt presset situation er det afgørende, at virksomhederne har forberedt sig, så de kan opretholde kritiske funktioner i tilstrækkelig grad og derigennem også kundernes og andre interessenters tillid.

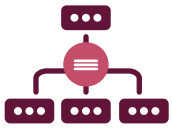
Det vil efter al sandsynlighed ikke være muligt at forberede sig til præcist det nedbrud, som faktisk indtræffer. Derfor er det både her og på de øvrige områder væsentligt at arbejde med hovedscenarier frem for (for) mange detaljerede scenarier, så anvendeligheden af scenarier og planer sikres.

Og uanset: Jo bedre forberedt virksomheden er, jo flere kort har den på hånden den dag, hvor nedbruddet faktisk sker.

3. Har virksomheden overblik over konsekvenserne af et nedbrud – også over tid?

En cyberstresstest giver konkret indblik i, hvad konsekvenserne er, når den almindelige IT-understøttelse ikke fungerer over længere tid. Og hvor flere kritiske forretningsfunktioner er ramt samtidig. Det, som f.eks. er et irritationsmoment på dag 1, bliver måske til en alvorlig mangel på dag 5. Andre funktioner kan måske bedre undværes i længere tid, eller kan bedre undværes på nogle tidspunkter end på andre. Cyberstresstesten viser, om virksomheden forstår effekter, konsekvenser og omkostninger ved nedbrud over tid godt nok til, at den kan skalere nødplanerne og den øvrige krisestyringsindsats til et tilstrækkeligt niveau.

Cyberstresstesten giver desuden myndigheder indsigt i virksomheders forventninger til udviklingen i konsekvenser over tid. Og dermed også en øget forståelse af, hvornår og hvordan et operationelt nedbrud ville kunne udvikle sig til at få systemiske konsekvenser. Den viden kan bruges til at tilrettelægge og prioritere myndighedsindsatsen fremadrettet, så eventuelle systemiske effekter kan håndteres bedst muligt.



Læring fra første cyberstresstest: Konsekvenserne udvikler sig over tid

Nedbruddets relativt lange varighed viste, at konsekvenserne af et nedbrud udvikler sig over tid. F.eks. må det forventes, at der sker ændringer i, hvordan og i hvor høj grad kunderne henvender sig til et pengeinstitut, som er ramt af et IT-nedbrud på henholdsvis dag 1 og f.eks. dag 5.

Derfor er det vigtigt på forhånd at have forholdt sig til, hvad effekterne vil være i forskellige hovedscenarier over tid. Det er samtidig vigtigt, at virksomhederne ikke kun vurderer konsekvenser (f.eks. økonomisk eller omdømmemæssigt tab) i omkostningsintervaller, men også forholder sig til, hvad der faktisk ville ske, hvem der ville blive berørt og hvordan. Dermed får man et oplyst grundlag for at forberede sig tilstrækkeligt på at håndtere konsekvenserne.

---

4. Er kommunikation en integreret del af nødplanlægningen og krisestyringen?

I en cyberstresstest skal virksomhederne forholde sig til, hvordan de vil kommunikere internt og eksternt, herunder til både kunder og offentligheden under et længerevarende nedbrud. Testen illustrerer, om den planlagte kommunikation understøtter nødplanerne og krisehåndteringen generelt. Er det f.eks. klart for kunderne, hvordan de skal forholde sig? Hvor mange kunder forventes at kontakte virksomhederne for at få hjælp til det, der ikke fungerer, som det plejer? Eller bare for at spørge, hvad der foregår? Hvor mange ressourcer har kundeservice brug for til at bistå kunderne? Og hvordan vil virksomheden håndtere omtale i både traditionelle og på sociale medier?

Læring fra første cyberstresstest: Kommunikation bliver afgørende, når virksomheden ikke kan levere de ydelser, den plejer

Virksomhederne blev også spurgt til, hvordan de ville håndtere kommunikationen under nedbruddet. Både til kunderne, offentligheden og andre interessenter. Og på forskellige platforme, herunder sociale medier.

Testen viste klart, at alle deltagerne var meget bevidste om, at vellykket kommunikation under en krise er afgørende for, at tilliden til virksomheden bevares. Det er vigtigt, at kommunikationen er afstemt mellem relevante parter og på forskellige medieplatforme for, at det lykkes. F.eks. hvornår og hvordan man melder ud, at der er tale om et cyberangreb, hvis det er det, der er tale om. Det er også vigtigt, at kommunikationen understøtter den

øvrige indsats, herunder nødplaner. Hvis nødplanen f.eks. forudsætter, at berørte kunder kan kontakte virksomheden, er det afgørende, både at kunderne får besked om det, og at der er tilstrækkelig kapacitet til at håndtere henvendelserne.

Forberedelse og test af kommunikationsindsatsen på forhånd er en væsentlig faktor givet det ekstreme tidspres under en krise. Det gælder på flere planer: **Strategi** – hvad vil virksomheden kommunikere hvornår. **Koordinering** – hvem skal budskaberne og timingen af dem være afstemt med både på forhånd og undervejs. **Konkrete planer og budskaber** – præfabrikerede og aftalte budskaber til hovedscenarier, så man ikke skal starte fra bunden, mens det "brænder".

Testen satte også fokus på, at sociale medier betyder, at det er langt sværere at styre fortællingen i en krise, end det var tidligere. Alle – utilfredse og bange kunder, influencere med egen dagsorden, internet-trolls mv. – har adgang til sociale medier. Og når noget først er skrevet, er det ekstremt vanskeligt at tilbagevise. Uanset om det er sandt eller ej. Denne nye virkelighed skal tænkes ind i kommunikationsstrategier og planer for, at indsatsen lykkes, så tilliden bevares.

5. Er virksomhedens beredskab tilstrækkeligt koordineret?

Endelig sætter cyberstresstest fokus på at udvikle et samlet beredskab, hvor forretningen, IT og kommunikation hænger sammen og understøtter hinanden. For IT-afdelingen kan ikke håndtere et omfattende, længerevarende IT-nedbrud alene. IT-afdelingen kan sørge for, at den almindelige IT-understøttelse bliver genoprettet så hurtigt som muligt. Men det er de forretningsvendte afdelinger frem for IT-afdelingen, som kan aktivere forretningsnødplanerne og derigennem f.eks. sikre, at en ramt banks kunder fortsat kan betale for varer i butikkerne, selvom bankens IT-systemer er ude af drift. Og det er kommunikationsafdelingen, der kan sikre, at kunderne og medierne får besked om, hvad der foregår, og hvordan de skal forholde sig. Endelig kræver det en samlet indsats at sikre, at IT-genopretning, forretningsnødplaner og kommunikation er koordineret - også med virksomhedens øverste ledelse. I en cyberstresstest stresses den samlede indsats i et konkret scenarie til det yderste for at belyse, hvor det kan gøres bedre.

Læring fra første cyberstresstest: Koordinering er en forudsætning for håndtering af omfattende, længerevarende IT-nedbrud

Testen handlede som nævnt om virksomhedernes håndtering af nedbruddet inden for forskellige indsatsområder.

Her viste testen klart, at effektiv håndtering forudsætter koordinering, også med eksterne parter som f.eks. leverandører. Det gælder på flere niveauer. F.eks. forudsætter genetablering af konkrete IT-systemer typisk, at den underliggende IT – servere, netværk mv. – er genetableret først. Det gælder også kommunikation: Hvis f.eks. én virksomhed giver oplysninger til offentligheden om årsagen til et nedbrud, kan andre ramte virksomheder ikke vælge at vente.

Derfor er det afgørende, at man har koordineret på forhånd og testet, at det virker. Det gælder internt i virksomhederne mellem forretning, IT og kommunikation, og det gælder mellem relevante parter, f.eks. leverandører.

Endelig skal håndteringen af omfattende, længerevarende IT-nedbrud forankres i virksomhedens samlede ledelse. Det er en forudsætning for tilstrækkelig koordinering på tværs.

6. Systemisk fokus i næste cyberstresstest

Den første cyberstresstest havde fokus på den enkelte virksomheds håndtering af et omfattende, længerevarende IT-nedbrud. Det har givet både deltagerne og myndighederne væsentlig læring.

Som beskrevet i det foregående ville et omfattende, længerevarende IT-nedbrud i virkeligheden også påvirke andre virksomheder meget hurtigt. Et sådant nedbrud ville også blive håndteret i et samarbejde mellem flere aktører, både andre finansielle virksomheder og myndighederne. Hvis en situation er tilstrækkelig alvorlig, vil FSOR's kriseberedskab blive aktiveret.

FSOR og FSOR's kriseberedskab: Finansielt Sektorforum for Operationel Robusthed (FSOR) er et offentlig-privat samarbejdsforum i den finansielle sektor initieret og drevet af Nationalbanken. FSOR's formål er at øge den operationelle robusthed på tværs af sektoren, herunder robustheden over for cyberangreb. FSOR har etableret et kriseberedskab på sektorniveau, som supplerer medlemmernes egne kriseplaner og det nationale kriseberedskab, NOST. Kriseberedskabet vil blive aktiveret i tilfælde af alvorlige operationelle forstyrrelser, som har potentiale til at påvirke den finansielle stabilitet.

Finanstilsynet vil gennemføre endnu en cyberstresstest. Formålet er denne gang at undersøge, hvordan et omfattende, længerevarende IT-nedbrud håndteres på tværs af aktører i sektoren og at kortlægge konsekvenser på sektorniveau. Da testen fokuserer på det finansielle system som helhed og konsekvenser på sektorniveau, gennemføres den i tæt samarbejde med Nationalbanken, som bl.a. har til opgave at sikre finansiel stabilitet.

Testen vil basere sig på et nedbrudsscenarie, som påvirker på tværs af den finansielle sektor. Det vil bl.a. give yderligere indblik i, hvilke værktøjer hos både virksomheder og myndigheder der egner sig til at håndtere operationelle nedbrud, og hvordan de bedst anvendes.

Testen er under planlægning og forventes gennemført i 2025.