Danmarks værn mod cyberkriser

Af **Joachim Finkielman**

Cyberangreb er allerede en realitet, som Danmark skal være forberedt på og kunne forsvare sig imod. Som et af verdens mest digitaliserede samfund er det særligt vigtigt for Danmark at være på vagt i cyberspace og klar til at håndtere cyberkriser.

Sårbarheden stiger i takt med afhængigheden af informationsteknologi (IT). I et af verdens mest digitaliserede samfund er én ting sikker: Cyberkrisen kommer, og den kan indtræffe når som helst, hvor som helst og på måder , vi ikke havde forudset. Vi har allerede set, hvor omfattende konsekvenserne kan være, da Mærsk i 2017 mistede i omegnen af to milliarder kroner, da et cyberangreb satte it-systemer ud af spil. Nok kan cyberangreb være kilden til en krise, men konsekvenserne vil formentlig være de samme og lige vidtgående som ved natur- eller menneskeskabte kriser.

Hvis man spørger, om Danmark er under angreb, er det simple - og måske for nogen overraskende - svar "ja!". Danmark angribes på daglig basis i cyberspace. Som et af de mest digitaliserede samfund i verden er det som sådan ikke overraskende. Angrebene er blevet "en ny normaltilstand" og rammer i øvrigt de fleste moderne samfund.

Heldigvis arbejdes der målrettet på at beskytte vores land blandt myndigheder, i det private erhvervsliv og på tværs af sektorer. Og heldigvis med en vis succes. Men hvad sker der, når angreb udvikler sig til en cyberkrise? Hvad sker der, hvis strømmen svigter, vandforsyning afbrydes eller dankortet sættes ud af spil? Har vi da et relevant beredskab?

Min påstand er, at vi i Danmark er godt rustet til at håndtere kriser. Også dem, der udløses i cyberspace. Men man skal aldrig undervurdere uvis-

Joachim Finkielman er vicedirektør i Beredskabsstyrelsen og chef for Myndighedsdivisionen samme sted. Han er uddannet cand.scient.pol. ved Københavns Universitet og har i en længere årrække arbejdet i Forsvarsministeriet, senest som kontorchef for forsvars- og sikkerhedspolitisk kontor.

hed og strategiske overraskelser. Verdenshistorien er fyldt med eksempler på kriser, der er opstået pludseligt og uforudsigeligt. Beredskabsstyrelsen arbejder med beredskabsplanlægning og krisestyring før, under og efter kriser, og det i tæt samarbejde med centrale offentlige og private aktører.

Store samfundsmæssige konsekvenser

Cyberkriser er et hurtigt voksende fænomen. Begrebet dækker over kriser, hvor it udgør et væsentligt element. Cyberkriser kan forårsages af bevidste handlinger – cyberangreb – men også af tekniske fejl. Center for Cybersikkerhed under Forsvarets Efterretningstjeneste deler cybertruslen fra bevidste handlinger op i fire kategorier: cyberspionage, cyberkriminalitet, cyberaktivisme, cyberterror. Alle fire kategorier har potentiale til at føre til en cyberkrise.

> **Danmark angribes på daglig basis i cyberspace. Angrebene er blevet "*a new normal*".**

Ud over disse tilsigtede aktiviteter kan også systemfejl skabe store cyberkriser for myndigheder og virksomheder. Disse opstår eksempelvis, når it-løsninger ikke er opdaterede. Det kan skyldes manglende tilpasninger, opgradering og/eller vedligeholdelse af eksempelvis specialudviklede it-løsninger, hvilket gør dem sårbare. Systemerne fejler i sig selv eller har svært ved at arbejde sammen med andre mere moderne systemer.

It-systemer, som understøtter telefoni, energi- og vandforsyning, kontrolsystemer i industrien eller transportinfrastrukturen har stor betydning for samfundsvigtige funktioner. I takt med, at stadigt flere infrastrukturområder benytter sig af digitale løsninger og tilkobles internettet, stiger sårbarheden og den potentielle rækkevidde af konsekvenser ved angreb eller nedbrud. Især fejl i eller angreb på industrielle styrings- og overvågningssystemer, som finder bred anvendelse i flere sektorer, har potentiale til at påvirke samfundet i omfattende grad. Her kan der eksempelvis være tale om, at strømforsyning, varmeforsyning, vandforsyning, internet, mobilnet med videre kan svigte. Togdriften, skibsfarten og luftfarten kan blive nødt til at indstille driften helt eller delvist. Hospitaler og andre sundhedsorganisationer kan få indskrænket mulighederne for at kunne udføre deres arbejde. Konsekvenserne kan også omfatte forstyrrelser i lønudbetaling, pensionsudbetaling, personregistrering, central virksomhedsregistrering, offentlig tinglysning, skatteopkrævning mv. Betalingsformidling og overførsler, værdipapirhandel med videre. kan blive utilgængelig i en periode. Alt i alt potentielt omfattende udfordringer på en bred vifte af områder.

Øvelse gør mester

Hvor vigtigt det er at beskæftige sig med fænomenet cyberkrise, blev bekræftet under den seneste nationale krisestyringsøvelse (KRISØV) 12. september 2019. KRISØV er en tilbagevendende øvelse, der hvert andet år træner centrale aktørers evne til at op-

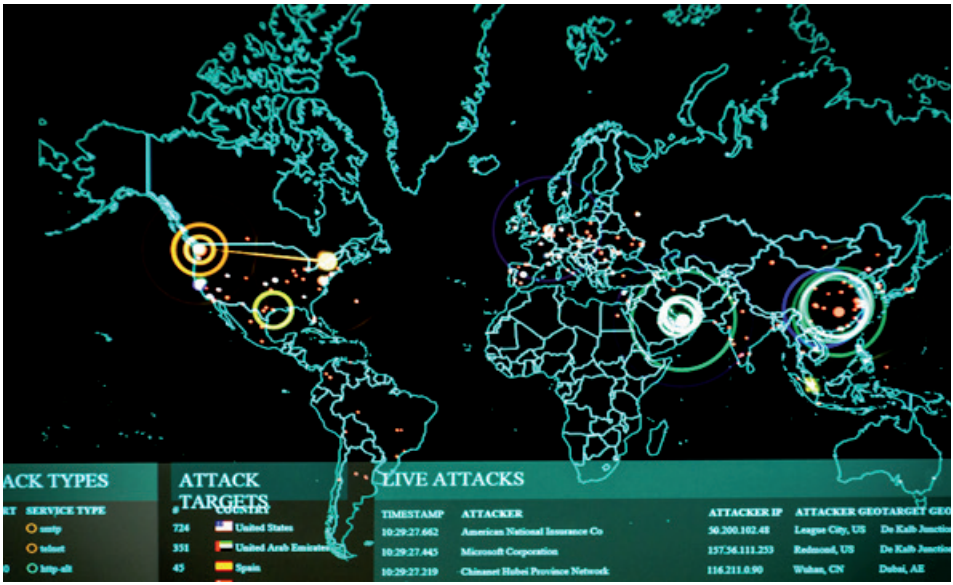

FOTO: Danmark udsættes dagligt for cyberangreb, hvilket stiller høje krav til beredskab og ikke mindst individuel adfærd. Her ses en amerikansk oversigt over cyberangreb på global plan 3. juni 2017.

(Foto: Joseph Eddins)

retholde og videreføre samfundsvigtige funktioner i en situation, hvor disse funktioner trues, svækkes, afbrydes eller ødelægges. KRISØV planlægges og ledes i fællesskab af Rigspolitiet og Beredskabsstyrelsen, og i dette års KRISØV deltog mere end 30 myndigheder og virksomheder.

Øvelsens fokus i år var primært håndtering af en kemisk ulykke, men i randen af ulykken var et scenarie, hvor ondsindede aktører forsøgte at udnytte fokus på den kemiske ulykke til at få adgang til blandt andet statslige it-systemer ved hjælp af såkaldte phishing-angreb. Deltagende myndigheder og virksomheder i KRISØV modtog simpelt konstruerede phishing-mails (svindelmails, hvor afsender udgiver sig for at være en anden for at franarre modtager information, red.), der lignede officielle henvendelser med information om den kemiske ulykke. Omkring en fjerdedel af modtagerne klikkede på det ondsindede link. I en virkelig situation ville mange myndigheder have været i vanskeligheder. Den første krise (kemisk) havde pludselig fået tilføjet en cyberdimension – som potentielt ville kunne udvikle krisesituationen eksponentielt.

En vigtig lektie er, at virksomheder, myndigheder og borgere skal være bevidste om god "it-hygiejne". Det betyder, at der skal vises omhu og arbej-

des med menneskers it-adfærd. Hvis man ikke er bevidst om sin egen adfærd, kan det at klikke på tvivlsomme links, bruge svage kodeord og genbruge kodeord flere steder have alvorlige konsekvenser.

Gode systemer afgør

Det var med afsæt i en logik om, at kriser kan opstå på baggrund af mange forskelligartede hændelser og udvikle sig i utallige retninger, at det danske krisestyringssystem blev designet. Det nationale krisestyringssystem er fleksibelt og kan anvendes ved alle former for større ulykker og katastrofer eller ved større planlagte begivenheder, for eksempel politiske topmøder, sportsbegivenheder med videre. Fælles for dem er, at der er tale om situationer, der skaber et behov for en særlig indsats. Nogle hændelser er så alvorlige eller omfattende, at der er behov for krisestyring på tværs af mange forskellige myndigheder, både på centralt og lokalt niveau. I sådanne tilfælde koordineres indsatsen inden for rammerne af det nationale krisestyringssystem.

Systemet er bygget op omkring en række tværgående krisestabe; fra kommandostadet i et indsatsområde hele vejen op til Regeringens Sikkerhedsudvalg med statsministeren i spidsen.

Myndigheder, der til dagligt har ansvaret for en opgave, har også ansvaret for opgaven under en større ulykke eller katastrofe. Det kaldes sektoransvar. Alle ministre skal sikre et forsvarligt beredskab inden for eget ressort, herunder løbende at overvåge risikobilledet inden for egen sektor.

Hvis en cyberkrise medfører et behov for national koordination, vil den Nationale Operative Stab (NOST) og Det Centrale Operative Kommunikationsberedskab (DCOK) blive samlet under ledelse af Rigspolitiet. Hensigten er at skabe overblik om udfordringer og indsatser, at understøtte myndigheders arbejde med at videreføre samfundet og koordinere den eksternt rettede kommunikationsindsats på tværs af myndighederne. Det er afgørende i en krise at sikre relevante, præcise og koordinerede handlingsanvisninger til befolkningen og medierne. Styrken i dette system er, at det ikke kun anvendes for cyberkriser, men alle former af kriser – også dem, vi ikke kender endnu.

Det brede samarbejde om kriser

Med så digitaliseret et samfund, som vi har, er der i Danmark i særlig høj grad brug for et robust nationalt rammeværk for at beskytte mod cyberkriser. I 2018 lancerede den daværende regering en ny national strategi for cyber- og informationssikkerhed, som skal binde den samlede indsats sammen. Hensigten er at øge den tekniske robusthed i den digitale infrastruktur, øge viden og kompetencer hos borgere, virksomheder og myndigheder og styrke den nationale koordinering og samarbejdet på området.

Statslige myndigheder, regioner og kommuner er forpligtet til at udarbejde en beredskabsplan. Beredskabsstyrelsen rådgiver og støtter arbejdet. Kodeordet er at planlægge, så – i princippet – alle typer af kriser kan håndteres, fordi der er en effektiv, kendt og indøvet struktur på plads, inden krisen

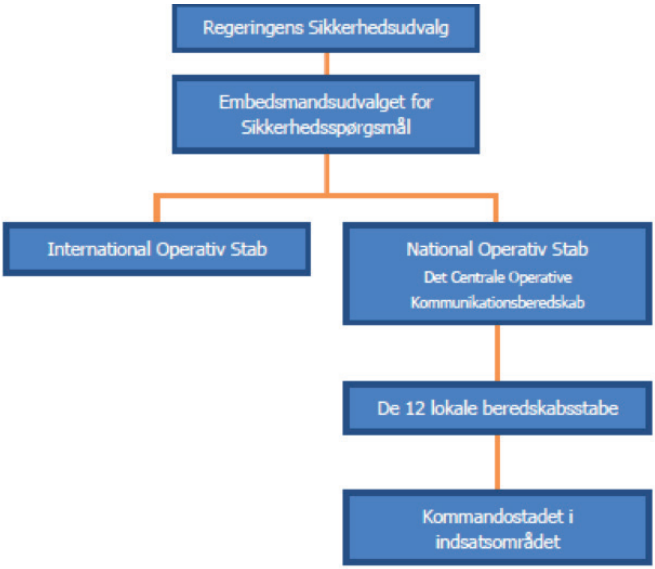

FOTO: Det danske beredskabs struktur til håndtering af kriser - også de cyberrelaterede.

(Foto: Beredskabsstyrelsen)

rammer. En beredskabsplan er et af de helt centrale elementer i krisehåndtering. Den kan endda hjælpe med at afværge, at en hændelse eller situation udvikler sig fra noget alvorligt til en krise. Det kræver dog, at alle aktører er bekendte med planen og deres rolle i den. Den fortrolighed med planen opnås gennem regelmæssige øvelser. Formålet med krisestyring er i sin kerne at få overblik, sætte retning og handle derefter, sådan at effekterne af krisen begrænses mest muligt, og genopretningen kan foregå så tidligt og smertefrit som muligt. Alle organisationer bør opbygge evnen til at krisestyre.

Det er ikke muligt at forberede sig på enhver type af krise, især fordi den næste krise godt kan være en, som man aldrig havde forventet. Det er imidlertid muligt at skabe en ramme og udvikle evner, som kan bruges under alle slags kriser. Med Beredskabsstyrelsens Nationale Risikobillede kan man med udgangspunkt i netop de risici, der er relevante for ens egen organisation, udarbejde et eget risikobillede. På denne måde kan det kortlægges, hvilke kriser der ses som mest relevante, samt definere, hvilke krisestyringskapaciteter der vil være nødvendige for at komme igennem disse kriser.

Én plan i hånden er bedre end…

Den bedste beredskabsplan nytter dog desværre ikke noget, hvis den ikke er tilgængelig under en krise. Især under cyberkriser kan det godt være, at IT-infrastrukturen ikke virker. Det er derfor en stor fordel, hvis relevante planer, telefonlister og actioncards på forhånd er fordelt i papirform.

Et solidt beredskab består af solide og velafprøvede relationer både horisontalt og vertikalt. Men også af kapaciteter, der kan bringes i anvendelse til at forebygge, håndtere og følge op på kriser. I en globaliseret verden, hvor kriser kan opstå på et splitsekund, over landegrænser og med potentielt katastrofale konsekvenser, må vi aldrig tro, at vi nu er gode nok til at håndtere kriser.

> **Vi vil blive overrasket på områder, hvor vi ikke havde drømt om at blive udfordret.**

Beredskab er en disciplin, som kontinuerligt skal drøftes, udvikles og afprøves. Det gælder nationalt som internationalt. Vi skal have et opdateret situationsbillede (og vi skal vide, hvad vi kigger efter), vi skal forebygge, hvor vi kan. Vi skal kunne varsle, når det, vi ser, afviger fra normalbilledet – og til de rigtige personer. Vi skal søge at afværge eller begrænse krisen og dens konsekvenser. Vi skal inddæmme udbredelsen af krisen, så længe den varer, og vi skal ikke mindst kunne genoprette hurtigt, når det er muligt.

Digitaliseringsgevinst?

Vores verden digitaliseres i en hastighed, der giver uanede muligheder og binder os sammen på en måde, der giver åbenlyse gevinster. Men digitaliseringen har også en pris, som udfordrer vores egen og fælles sikkerhed. Den selvfølgelighed, hvormed vi kommunikerer med hinanden og den lette transaktion, der foregår mellem os, er så indgroet en del af dagligdagen både herhjemme og internationalt, at vi let tager for givet, at ting gnidningsfrit kan lade sig gøre og håndteres. Denne selvsamme netværkstilgang gør os utroligt sårbare, særligt overfor cyberkriser. Det stiller umådeligt store krav til at sætte fokus på cyber- og it-sikkerhed inden for den enkelte og på tværs af sektorer. Derfor rækker Strategi for Cyber- og Informationssikkerhed 2018-2021 også bredt ud. Digitaliseringen stiller naturligvis også store krav til Beredskabsstyrelsens evne til at rådgive om og udvikle beredskabsplanlægningen, så den er relevant og anvendelig også i de kommende år. Det er vi i gang med, og det vil være et arbejde, der aldrig kan tilendebringes, da udfordringerne er dynamiske.

Der er ingen tvivl om, at vi som andre bliver udfordret af kriser fremadrettet. Vi vil blive overrasket på områder, hvor vi ikke havde drømt om at blive udfordret. I de situationer er det vigtigt at vide, hvem der gør hvad, og hvordan. Som nævnt er en god beredskabsplan ikke i sig selv et værn mod krisen, men den kan give en ramme for, hvordan krisen systematisk kan håndteres. Og sådan en plan skal øves jævnligt, hvis den skal fungere.