Cybertruslen: Kompleksitet der kræver (an)svar

Christensen, Kristoffer Kjærgaard; Petersen, Karen Lund

Publication date:
2017

TÆNK RET SIKKERHED

Af Kristoffer Kjærgaard Christensen og Karen Lund Petersen

Cybertruslen: Kompleksitet der kræver (an)svar

Cybertruslen regnes i dag for den absolut største trussel både i det private erhvervsliv og sikkerhedspolitisk. På trods af dette er der i Danmark et fravær af både koordinerende myndighed og en åben politisk prioritering på området. Danmark har i modsætning til mange andre lande fravalgt at have en centralt koordinerende myndighed på cyberområdet samt en klar definition af, hvilke industrier og funktioner, der udgør rigets kritiske infrastruktur.

Et meget stort ansvar for rigets cybersikkerhed ligger derfor ude i virksomhederne og organisationerne, nationale såvel som internationale, og der er kort sagt stor forvirring på området. Hvem skal gøre hvad, hvornår?

De manglende prioriteringer og den manglende koordinering øger Danmarks sårbarhed over for cyberangreb. Samtidig svækkes det danske demokrati, da grænserne for dansk sikkerhedspolitik forbliver usagte og uden for den demokratiske offentligheds skue.

I dette brief opridses de nuværende rammer og udfordringer for danske virksomheder og giver anbefalinger til, hvor der kan sættes ind mod cybertruslen.

ABSOLUT STØRSTE TRUSSEL

Flere undersøgelser viser, at private virksomheder – uanset sektor – i dag anser truslen mod og gennem informations- og kommunikations-teknologi (IKT- eller cybertruslen) som den absolut største. Amerikanske og europæiske efterretningstjenester vurderer desuden truslen som en verdensomspændende udfordring, og NATO har senest udpeget cyberspace som et selvstændigt domæne for krigsførelse.

På trods af denne enighed om vigtigheden af problemet er der langt fra enighed om, hvilke midler der skal til for at bekæmpe truslen.

Truslens komplekse, dynamiske og diffuse karakter gør den svær at udpege og dermed styre. Informations- og kommunikationsteknologi er overalt: Den overskrider ikke kun de nationale jurisdiktioner, men har i den digitale tidsalder fundet vej ind i 'det private rum'. Vores kritiske infrastruktur, private virksomheder og de mest intime aspekter af vores daglige liv er påvirket af

informations- og kommunikationsteknologi og det hastigt voksende 'Internet of Things'.

Denne udvikling udvider drastisk de sikkerhedspolitiske sårbarheder og antallet af potentielle mål – fra stater til private virksomheder og individuelle brugere.

Vi ved ikke, hvor cybertruslen kommer fra næste gang, eller hvem/hvad der er målet. Er det stater eller individer, der angriber? Ligger der politiske, økonomiske eller helt tredje motiver bag?

Denne usikkerhed gør klassisk politisk styring gennem lovgivning meget vanskelig. Bekæmpelse af cybertruslen kræver i stedet, at sikkerhedspolitik og kriminalitetsbekæmpelse tænkes ud over den klassiske politimæssige og forsvarspolitiske styring.

ANBEFALINGER

- At der skabes et rum for prioritering og strategisk tænkning i forhold til cybertruslen.
- At civile organisationer og virksomheder i Danmark blander sig mere i debatten og udvikler fælles politikker og normer på området.
- At der satses på læring og uddannelse i organisationen for at sikre dialog og "oversættelse" mellem det strategiske og det tekniske niveau.

Effektiv bekæmpelse af cybertruslen er kort fortalt afhængig af, at virksomheder og organisationer frivilligt bidrager ved konstant at forholde sig til truslens omskiftelige karakter og egenhændigt gør en aktiv indsats.

Det er således ikke længere nok at forholde sig til ny lovgivning, men truslens karakter kræver samfundsmæssig ansvarlighed og selvregulering hos en bred vifte af samfundets organisationer.

Mere end nogensinde før ser vi således i dag et opbrud i grænserne mellem statens ansvar for nationens *sikkerhed* og borgerens *ret* til beskyttelse; grænsen mellem den offentlige og den civile sfære.

I det følgende vil vi opridse de rammer og udfordringer som danske virksomheder står overfor i relation til cybertruslen og give tre bud på hvor disse organisationer og virksomheder kan og bør sætte ind.

DEN INSTITUTIONELLE KONTEKST

De fleste vestlige lande, heriblandt Danmark, har taget en række politiske initiativer for at imødekomme det øgede behov for cybersikkerhed og derved sikre en fortsat udvikling af vores informations- og kommunikationsteknologi.

Lovgivningen er blevet skærpet og nye myndigheder er etableret.

"Forskellen i forhold til tidligere er et mere diffust og uforudsigeligt trusselsbillede. Angrebsfladen på IT-siden er hyperdynamisk og øges af nye teknologier samt forventningen om, at vores digitale identitet er tilgængelig 24/7/365 – uanset hvor på kloden vi befinder os." Thomas Baltzer Jensen, Chief Operational Risk Officer i Danmarks Nationalbank.

I Danmark fordeles opgaverne primært mellem Center for Cybersikkerhed (CfCS), Politiets Efterretningstjeneste (PET) og Nationalt Cyber Crime Center (NC_3) – og i mindre grad også Digitaliseringsstyrelsen og Statens IT (se figur på næste side).

Denne opdeling beror i vid udstrækning på muligheden for at opretholde den klassiske

CfCS: National IT-sikkerhedsmyndighed	PET: National sikkerhedsmyndighed	NC3: Politiets cyber crime center	Digitaliseringsstyrelsen: Rådgivning af statslige myndigheder
• Fokus på særligt avancerede trusler fra udlandet mod kritisk infrastruktur • Nationalt kompetencercenter på cybersikkerhedsområdet	• Fokus på trusler mod nationens sikkerhed og fysisk sikring af information • IT-sikkerhedsmyndighed på Justitsministeriets område	• Fokus på forebyggelse, efterforskning og opklaring af IT-kriminalitet mod borgere og SMV'er	• Fokus på at statslige myndigheder lever op til obligatoriske principper • Publicerer materiale om informationssikkerhed rettet mod borgere og statslige myndigheder

adskillelse mellem national sikkerhed (CfCS og PET) og kriminalitetsbekæmpelse (NC3) og tilstræber en kategorisering og fordeling af opgaverne derefter.

Det primære fokus for Center for Cybersikkerhed er beskyttelse af den kritiske infrastruktur mod "avancerede vedvarende trusler" (såkaldte APT-angreb) og andre sofistikerede, eksterne trusler. Centret tager sig af trusler mod nationens sikkerhed, som typisk kommer fra andre stater eller statsstøttede aktører. Mindre avancerede angreb og angreb med kriminelle hensigter betragtes som et anliggende for politiet og organisationerne selv.

"Cyber/Communications Security remains the greatest security concern facing Fortune 1000 companies in 2016", 2016 Survey of Fortune 1000 Companies, Securitas

Cybertruslen er således fra statens side langt hen ad vejen defineret ved aktøren – om det er fjendtlige stater eller statsstøttede grupper eller blot kriminelle, der står bag angrebet.

Modsat flere andre lande har vi i Danmark ikke én central koordinerende myndighed på cyber-området, men det er op til den enkelte organisation at vurdere karakteren og omfanget af sikkerhedshændelser: Med andre ord at afgøre om en given hændelse i første omgang skal kategoriseres som en sikkerhedshændelse og et myndighedsanliggende, og dernæst hvilken myndighed der i så fald skal rettes henvendelse til. I denne danske model er det således virksomheden/organisationen, som primært har ansvaret for at lave den konkrete fortolkning af sikkerhedshændelser.

Ud over at vi i Danmark ikke har én central og koordinerede myndighed på cyberområdet, har vi modsat mange andre lande heller ikke en officiel stillingtagen til, hvad staten ser som vigtige samfundsfunktioner. Vi har med andre ord ingen klar definition af, hvilke industrier og funktioner der udgør den *kritiske infrastruktur*.

"Som borger og som virksomhed er det ofte svært at finde ud af, hvor man skal henvende sig, og hvem der har ansvaret. Folk må ofte gå forgæves på deres lokale politistation, og det er for mange svært at kende forskellen på de mange aktører som NC3, Center for Cybersikkerhed, private aktører med mere". Rasmus Theede, formand for Rådet for Digital Sikkerhed

Forsvarets Efterretningstjeneste skriver i 2013, at der her er tale om "energi-, transport-, forsynings, finans- og kommunikationsområdet samt

funktioner, som har stor økonomisk betydning for samfundet.", mens Beredskabsstyrelsen i 2016 definerer den kritiske infrastruktur som "fx veje, jernbaner, teleforbindelser, sundhedsvæsnet og andre anlæg og funktioner, som er nødvendige for at samfundet kan fungere."

I stedet for kritisk infrastruktur er sektoransvaret i centrum for cyberberedskabet. Dvs. det forhold, at det er de pågældende myndigheder inden for det enkelte ressortområde, som har ansvar for at håndtere fremtidige hændelser. Dette betyder i almindelighed, at fokus er på re-aktion (beredskab) og ikke på den koordinerede forebyggende indsats.

Fraværet af en koordinerende myndighed samt en åben politisk prioritering af, hvilke samfundsfunktioner, som er vigtige, gør ansvarsfordelingen mellem myndigheder og civile organisationer uklar. Det skaber kort sagt forvirring om, hvem der bør gøre hvad og med hvilket ansvar til følge.

Virksomheder er mere eller mindre overladt til egen dømmekraft i relation til vurderingen af samfundsmæssige og sikkerhedspolitiske behov for viden og handling. Man risikerer dermed, at vigtig viden ikke bliver delt.

En manglende prioritering af de kritiske samfundsfunktioner har desuden negative demokratiske effekter, da grænserne for dansk sikkerhedspolitik forbliver usagt og uden for den demokratiske offentligheds skue.

HVORI BESTÅR OPGAVEN FOR VIRKSOMHEDER OG ORGANISATIONER?

Det er almindeligvis vanskeligt at skelne mellem forskellige IKT-relaterede sikkerhedsbrud, såsom avancerede hackerangreb fra andre nationer, datatyveri, hærværk og teknologiske svigt.

Det er kort sagt forbundet med stort besvær og betydelige omkostninger at afgøre, 'hvem' og 'hvor' truslen kommer fra. Fordi analysen ofte er vanskelig og meget dyr, er det heller ikke altid i virksomhedens eller organisationens interesse at foretage den gennemgribende analyse af en hændelse og derved fastslå aktører bag.

Det interessante for virksomheden eller organisationen er snarere at vurdere, hvori sårbarhederne består, og hvilke konsekvenser eventuelle angreb vil have for den fremtidige drift, kommende projekter og omdømme.

I virksomhederne er der således mindre fokus på trusselsaktørerne og mere fokus på metoderne og sårbarhederne i forbindelse med en hændelse, da der her lettest, billigst og mest effektivt kan sættes ind med forbedringer af beredskabet.

Sårbarheder og trusler relateret til IKT er således et vilkår, som langt hen ad vejen imødekommes ved at sikre systemer og arbejdsgange samt ved at risikovurdere nye forretninger og initiativer – alt i overensstemmelse med den enkelte virksomheds strategiske prioriteter og risikoappetit.

De virksomheder, der opererer globalt, ser derfor heller ikke kun på trusler mod deres danske netværk eller på den danske eller europæiske lovgivning, men vurderer de bredere politiske risici.

Virksomhederne divergerer således fra myndighederne i denne henseende. Det er ikke overraskende, at myndighedernes fokus defineres af hensynet til nationen, men i og med at cybertruslen for virksomhederne ikke defineres af nationale grænser, kan de ikke alene forlade sig på samarbejdet med myndighederne. Hvilke myndigheder skal man henvende sig til? Og ikke mindst til hvilken nytte? Det er derfor vigtigt, at

virksomhederne også selv tager initiativ på området.

Selvom virksomhedens egne procedurer og teknikker potentielt kan sikres og teknisk forbedres, er der stadig nogle grundlæggende strategiske udfordringer.

Som en undersøgelse fra PWC viser, anser danske virksomheder truslen fra organiserede kriminelle hackere som størst – primært pga. de potentielt store økonomiske tab.

Lovgivning på cyberområdet bekymrer i noget mindre grad. (se PWCs Cyber Crime Survey 2016) Dette syn på regulering må dog forventes at ændre sig i de kommende år; dels pga. den intensiverede EU-indsats på persondata-beskyttelsesområdet og dels på grund af frygten for, hvad der populært kaldes 'cybernationalisme', altså det fænomen at regeringer verden over søger at beskytte data ved at etablere nationalt kontrollerede grænser for databehandling.

"Security is not simply a CIO, CSO, or IT department issue… It is a responsibility that must be shared amongst all employees, and CEOs and board members must proactively mitigate future challenges." AT&T Vice Director, John Donnovan 2015

Konsekvenserne af en sådan politik er potentielt negative for virksomheder, der opererer på det globale marked. Som litteraturen ofte peger på, er nationale lovgivninger på cyberområdet ikke altid kompatible, og det kan derfor være svært at etablere en praksis for brugen af teknologi.

Eksempelvis har Rusland vedtaget en anti-krypteringslov (Yarovya-lov fra 2016), som stiller nogle krav til virksomhederne, der er i direkte modstrid med europæiske og amerikanske regler for privatlivsbeskyttelse.

Foruden kompatibilitetsproblemet kan visse former for lovgivning og teknologiske løsninger potentielt få meget vidtrækkende betydning for hele sektorer (e-handel og tele-branchen er oplagte eksempler).

Et godt eksempel er debatten om efterretningstjenesternes ret til i tilfælde af kriminalitet eller terrorisme at have adgang til en 'bagdør' til krypteret indhold eller 'logget' information hos teleselskaber og internetudbydere. En sådan lovgivning vil kunne få vidtrækkende konsekvenser for tele- og teknologivirksomheder og deres brugere verden over.

Vi står her over for et klassisk dilemma mellem sikkerhed på den ene side og frihed (og velstand) på den anden – med virksomheder og organisationer stående i centrum. Hvor meget sikkerhed skal vi søge at opnå via overvågning og andre initiativer? Og hvor meget frihed og frihandel er vi villige til at opgive i sikkerhedens navn? Som beskrevet nedenfor i vores anbefalinger er det vigtigt, at danske virksomheder tager stilling til dette spørgsmål og har en stemme i debatten.

Ud over at pege på udfordringer med øget IT-kriminalitet viser PWCs undersøgelser, at relativt mange af de adspurgte efterspørger klarere prioriteringer af udfordringerne hos topledelsen.

I USA svarer 75% således, at cybersikkerhed ikke anses som et anliggende for bestyrelsen. I stedet bliver cybertruslen oftest set som et 'management' problem, der skal og kan håndteres i IT-, Sikkerheds- og HR-afdelingerne. Dette skaber ofte problemer med silo-tænkning

og manglende strategisk stillingtagen til problemets karakter og omfang.

HVAD KAN DER GØRES?

Udfordringerne for virksomhederne er således mange. Men selvom forebyggelse, resiliens og robusthed er de gængse svar på, hvordan vi kan og skal os forholde til nye og mere uforudsigelige trusler, er det vigtigt at holde sig for øje, at vi aldrig hverken kan eller skal forebygge fuldstændigt. Det vil være grundlæggende i modstrid med vores tro på privatlivets fred og retten til selvbestemmelse. Vi skal i stedet handle klogere inden for rammerne af vores liberale demokrati.

I det følgende vil vi pege på tre områder, hvor virksomheder og organisationer kan og bør sætte ind for at navigere i det nye trusselsbillede.

ANBEFALING: PRIORITÉR OG TÆNK STRATEGISK I HELE ORGANISATIONEN

På grund af cybertruslens kompleksitet berører den hele organisationen. Denne kompleksitet gør strategiske beslutninger og prioriteringer på topledderniveau meget vigtige.

Ved at træffe beslutninger om cyber- og informationssikkerhed på strategisk niveau og på baggrund af strategiske risiko- og trusselsvurderinger kan en integration af sikkerhedsbeslutningerne i organisations generelle arbejde sikres.

Karakteren af risikobeslutningen er dog ikke den samme som med andre typer af risici. På grund af den usikkerhed, som er forbundet med cybertruslen, er det nærmest umuligt af kalkulere sandsynligheden og konsekvenserne af cyberhændelser. Opgaven er således ikke at beregne og på den baggrund kontrollere, men at tage oplyste og bevidste valg baseret på forskellige mulige fremtidsscenarier. Risikohåndtering på cyberområdet kræver således strategiske og ledelsesmæssige valg.

Dette handler ikke nødvendigvis om flere midler, men om at skabe rammerne for en mere holistisk tilgang til arbejdet med cyber- og informationssikkerhed. Organisationens prioriteringer og linje skal være klar.

> *"Boards can hold executive management accountable for evaluating current cybersecurity risks and maintaining response plans by making cybersecurity debriefings a regular agenda item at board meetings."*
> *Harvard Business Review 2017*

Et råd kunne være at designe processer på tværs af organisationen, der sikrer samtænkning og refleksion i forhold til de forskellige dele af virksomheden, som er berørt. I denne proces vil man ikke blot sikre den rette form for risikohåndtering, men også undgå den form for silotænkning inden for Sikkerheds-, Risiko-, IT- og HR-afdelingerne, som generelt er en hindring for at finde løsninger på udfordringer angående cyber- og informationssikkerhed.

ANBEFALING: TAG EJERSKAB FOR DEN POLITISKE UDVIKLING

På grund at den sikkerhedspolitiske karakter af cybertruslen er det politiske pres på organisationer og virksomheder stort – og det må forventes at stige. I den forbindelse ser vi ikke blot en øget regulering på området, men også en højere grad af italesættelse af virksomheders og organisationers ansvar.

Særligt for større virksomheder og organisationer kan dette fokus få betydning af omdømmemæssig karakter.

Desuden er området så centralt for danske virksomheders og organisationers fremtidige muligheder for at handle, at det ikke er tilrådeligt at have en afventende position i forhold til lovgivning og normudvikling på området.

Gennem samarbejde på tværs af industrier er det muligt at sætte egne industrielle normer for håndteringen af truslerne – uden for det politiske system – og derved være både dags-ordenssættende og beredte.

Et godt eksempel på dette er en række større teknologivirksomheders arbejde med at forme dagsordenen for transparency og den principielle stillingtagen til dataudlevering til myndig-hederne.

Cybernationalisme er som nævnt ovenfor en reel trussel mod frihandel og et spørgsmål, som efter alt at dømme vil blive mere aktuelt de kommende år. På linje med selvstyringsinitiativer på andre områder er det også her muligt at etablere frivillige standarder og normsystemer på tværs af nationale skel og derved undgå overregulering.

Den udbredte anvendelse af frivillige rapporterings- og kontrolsystemer anvendes i stigende grad som værktøjer til selvregulering blandt virksomheder. Bæredygtighedsmål og rapportering om Corporate Social Responsibility er blot et par eksempler på sådanne vigtige værktøjer til kommunikation og styring af nye og uforudsigelige risici. En anden vej er en stigende brug af standarder som f.eks. ISO 27000-standarderne.

"Over 80 af de adspurgte virksomheder forventer, at dataanalyse vil have en væsentlig indflydelse på deres beslutningsprocesser om fem år. De danske virksomheder stiller sig relativt kritiske over for deres nuværende kompetenceniveau inden for dataanalyse."
PWC 2017

Disse rapporteringssystemer og selvpålagte regler er i dag anset som normer, der definerer den ansvarlige virksomheder. Selv om CSR-rapportering ofte kritiseres for blot at være en rapporteringsmekanisme for store virksomheder til at vise og annoncere alle de gode ting, de gør, snarere end at være en kerneaktivitet i virksomheden, er CSR stadig en vigtig norm, der tvinger virksomheder til at kunne forsvare deres handlinger moralsk.

I relation til cyberområdet kan virksomheder og organisationer med fordel bygge videre på deres allerede eksisterende internationale samarbejder i bestræbelserne på at modarbejde tendenserne til cybernationalisme.

I Danmark har vi f.eks. senest set et initiativ i den finansielle sektor til normregulering på cyberområdet i Norden - det såkaldte Nordic Financial CERT. Overordnet set giver den dynamiske teknologiske udvikling større spillerum for virksomhederne i forhold til at præge dagsordenen modsat reguleringens mere træge karakter.

ANBEFALING: SKAB MULIGHEDER FOR VIDENSDELING OG KOMPETENCEUDVIK-LING

Cyber- og informationssikkerhed fremstår ofte som komplekse tekniske problemstillinger, der kan være nærmest utilgængelige uden for specialiserede kredse. Dette skaber en følelse af afmagt.

For at de to andre mål kan opfyldes, er det vigtigt, at denne afmagt afmonteres, og der skabes et læringsrum om cyber- og informationssikkerhed. Dette skal være et læringsrum, der befordrer dialog og sund politisk, økonomisk og strategisk tænkning.

For det første er det helt grundlæggende nødvendigt at sikre, at de rette kompetencer er til stede i organisationen. Det er nødvendigt med såvel strategiske og økonomiske som tekniske og operative kompetencer for at kunne navigere i den komplekse virkelighed, som præger cyber- og informationssikkerhed.

For det andet er der særligt behov for at skabe kompetencer internt i organisationen, som gør det muligt at oversætte konkrete, tekniske og operationelle, udfordringer til det strategiske niveau – og omvendt. Dette handler ikke så meget om, at beslutningstagerne skal have specifikke tekniske/operationelle kompetencer. Det handler også om, at det tekniskvidende personale bliver uddannet til at forstå, hvordan deres valg og beslutninger hænger sammen med de strategiske. Dermed kan de være med til at sikre et informeret grundlag for den strategiske kurs i virksomheden. Denne oversættelse og vidensdeling er med andre ord essentiel for at sikre sammenhængen mellem de strategiske og de operative beslutninger.

Sidst, men ikke mindst, er der behov for en større grad af erfaringsudveksling og informationsdeling organisationerne imellem. Gennem samarbejde er der for alvor mulighed for at styrke organisationernes viden og kompetencer. Da vi i Danmark ikke har en central koordinerende myndighed på cyberområdet kræver styrket informationsdeling også privat initiativ og en styrkelse af de eksisterende private netværk.

FORFATTERNE

Maj 2017

Ph.d.-stipendiat Kristoffer Kjærgaard Christensen (kk@ifs.ku.dk), Institut for Statskundskab, Københavns Universitet

Lektor Karen Lund Petersen (klp@ifs.ku.dk), Institut for Statskundskab, Københavns Universitet