Hackertruslen mod Danmark

En analyse blandt IDAs it-professionelle

Februar 2019

Hackertruslen mod Danmark

Resume

Danmark er et af de mest digitaliserede lande i verden. Det giver os en masse muligheder, men det giver os også en masse udfordringer. Udfordringer som vi er forpligtet til at tage seriøst ansvar for. Med digitalisering følger risikoen for at blive hacket af ondsindede kræfter. Det er derfor blevet et vilkår, at vil man digitalisering er man også nødsaget til at stille med et seriøst værn mod hackerne. For de dygtige. Rigtig dygtige.

I nærværende analyse har IDA bedt sine it-professionelle medlemmer om at vurdere hvor høj hackertruslen fra forskellige aktører er mod i) deres egen arbejdsplads, ii) Danmarks infrastruktur og iii) Danmarks offentlige institutioner. Derudover er de it-professionelle blevet bedt om at tage stilling til, hvilke organer der er mest kompetent til at håndtere hackertruslen mod Danmark.

Analysens resultater

Analysen viser for det første, at der ifølge IDAs it-professionelle medlemmer er en hackertrussel mod Danmark. Truslen mod deres egen arbejdsplads er særlig høj fra organiseret kriminelle, imens det i høj grad er fremmede stater, der hackertruer den danske infrastruktur og de danske offentlige institutioner.

Med den omfattende digitalisering af den offentlige danske sektor, har de offentlige institutioner en særlig forpligtelse til at sikre, at værnet mod hackere er på sit absolut højeste. Af samme årsag er det afgørende, at den offentlige sektor har adgang til de rette kompetencer. Og i den forbindelse er det bekymrende, at analysen viser, at ca. hver tredje it-professionel i den offentlige sektor mener, at det er vanskeligt at rekruttere it-kompetencer indenfor sikkerhed/security.

Analysen viser endvidere, at Forsvarets Efterretningstjeneste ud af af de eksisterende organer betragtes, som det bedste til at håndtere cybertruslen mod Danmark. Men 65 pct. af de it-professionelle mener dog, at det vil være en god ide at oprette et råd baseret på civile aktører, offentlige myndigheder, forskere og virksomheder, hvilket har til opgave at overvåge cyberangreb mod danske virksomheder og offentlige institutioner samt advare og rådgive (dette efter Hollandsk model).

Indhold

Er 600 mio. kr. til cyberforsvar nok?

I Finansloven for 2018 blev der afsat 100 mio. kroner til udmøntningen af den nationale strategi for cyber- og informationssikkerhed. De 100 mio. kroner skal fordeles over en 4-årig periode, og skal ruste Danmark bedre mod it-kriminalitet og hackerangreb. Derudover blev der med forsvarsforliget 2018-2023 afsat 500 mio. kroner til en pulje, som skal gå til it- og cybersikkerhed.

Hver anden it-professionel mener, at 600 mio. kr. til cyberforsvar er for lidt

IDA har bedt sine it-professionelle medlemmer vurdere, hvorvidt 600 mio. kr. er nok til at styrke Danmark cyber- og informationssikkerhed. Svaret ses i *tabel 1* nedenfor.

Hver anden it-professionel mener, at 600 mio. kr. er *for lidt* eller *alt for lidt* til at styrke Danmarks cyber- og informationssikkerhed. Hver 10. mener, at det er tilpas, imens kun 2 pct. mener, at det er for meget eller alt for meget. Næsten 40 pct. svarer *ved ikke*, hvilket indikerer, at spørgsmålet kan være vanskeligt at svare på.

Tabel 1. Er 600 mio. kr. for lidt, tilpas eller for meget til at styrke Danmarks cyber- og informationssikkerhed?

	Antal	Procent
Alt for lidt	109	23 %
For lidt	125	27 %
Tilpas	47	10 %
Lidt for meget	6	1 %
Alt for meget	5	1 %
Ved ikke	175	38 %
I alt	467	100 %

Kilde: IDA Analyse (2019): Hackertruslen mod Danmark – analyse blandt IDAs it-professionelle

Hvorvidt en pulje penge er tilstrækkelig, er meget afhængig af, hvad de bruges på. Og her er IDAs politiske anbefalinger, at de 600 mio. kroner blandt andet bruges til:

- At forbedre sikkerheden i praksis, herunder øremærke en stor andel af puljen til at forbedre kompetencer og viden både i den offentlige og i den private sektor[1] på både ledelses- og medarbejderniveau. Der er både tale om behov for kompetenceløft og mange steder også en kulturændring.

- At anvendes til at styrke civilsamfundets robusthed overfor cyberangreb, herunder til virksomheder og kritisk infrastruktur.

[1] Jf. udmeldingen fra Digitaliseringsstyrelsen og Center for Cybersikkerhed "Cyberforsvar, der virker" fra januar 2017.

Hvem hackertruer Danmark?

Hackertruslen mod Danmark har i takt med den stigende digitalisering kun fået mere og mere bevågenhed. Af samme årsag udgiver Center for Cybersikkerhed hvert år en national trusselsvurdering. I maj 2018 udkom den på nuværende tidspunkt seneste vurdering, og heri fremgår det, at truslen mod Danmark er størst fra hhv. cyberspionage og cyberkriminalitet. Vurderingens hovedkonklusioner fremgår desuden af *boks 1* nedenfor.

Boks 1: Hovedvurdering fra Trusselsvurdering: Cybertruslen mod Danmark 2018

- Truslen fra cyberspionage er MEGET HØJ. Truslen er især rettet mod danske myndigheder, som har oplysninger, der er strategisk, politisk eller økonomisk værdifulde for fremmede stater. Visse stater udfører også cyberspionage mod danske virksomheder. Stater gør generelt mere for at skjule deres cyberspionage.

- Truslen fra cyberkriminalitet er MEGET HØJ. Cyberkriminalitet er et globalt fænomen, der også rammer danske myndigheder, virksomheder og borgere. Der er særligt en betydelig trussel fra cyberkriminalitet, der sigter mod at afpresse penge fra myndigheder, virksomheder og borgere. Der er cyberkriminelle netværk, der arbejder organiseret og langsigtet, og statsstøttede hackere står sandsynligvis også bag cyberkriminalitet.

- Truslen fra cyberaktivisme er MIDDEL. Cyberaktivister retter sjældent fokus på danske myndigheder og virksomheder. Nogle hackergrupper og individer i cyberaktivistiske netværk har dog væsentlige evner og ressourcer til at udføre cyberangreb. Det er sandsynligt, at stater også anvender visse cyberaktivistiske grupper som dække i forsøg på at påvirke meningsdannelsen i andre lande.

- Truslen fra cyberterror er LAV. Militante ekstremister har begrænsede evner og ressourcer til at udføre alvorlige cyberangreb. Selv om de i få tilfælde har ytret interesse for at udføre cyberterror, har de aktuelt ikke kapacitet til dette.

- Visse stater bruger cyberangreb til at styrke deres magtposition. Det gælder bl.a. anvendelsen af destruktive cyberangreb og hack og læk af politisk følsomt materiale. Danske virksomheder og organisationer er udsat for en større risiko for destruktive cyberangreb, hvis de er til stede i visse konfliktområder.

Kilde: Trusselsvurderingsenheden ved Center for Cybersikkerhed (maj 2018): "Trusselsvurdering – Cybertruslen mod Danmark"

33 pct.: Hackertruslen fra organiseret kriminalitet mod danske virksomheder er høj

IDA har bedt sine it-professionelle medlemmer om at vurdere, hackertruslen mod deres egen arbejdsplads. Resultatet heraf fremgår af *tabel 2*. Ca. hver tredje mener, at truslen fra i) fremmede stater og ii) organiseret kriminalitet er høj. Omkring hver tredje vurderer, at truslen fra organiseret kriminalitet, politiske/ideologiske hackere og interne forhold er middel. Og endelig mener 50 pct. og 41 pct., at truslen mod deres egen arbejdsplads fra hhv. terrororganisationer og interne forhold er lav.

Tabel 2. Hvordan vurderer du hackertruslen mod din egen organisations/virksomheds datasikkerhed fra?

	Lav	Middel	Høj	Ved ikke	I alt
Fremmede stater	34 %	23 %	29 %	13 %	100 %
Terrororganisationer	50 %	19 %	15 %	16 %	100 %
Organiseret kriminalitet	20 %	34 %	33 %	13 %	100 %
Politiske/ideologiske hackere	37 %	31 %	18 %	14 %	100 %
Interne trusler	41 %	35 %	10 %	14 %	100 %
Andet	16 %	18 %	9 %	57 %	100 %

Kilde: IDA Analyse (2019): Hackertruslen mod Danmark – analyse blandt IDAs it-professionelle
Note: n = 467

Fordeles resultaterne fra tabel 2 på offentlig og privat sektor, ses det, at IDAs it-professionelle i de to sektorer er overvejende enige i deres vurdering af hackertruslen mod deres egne arbejdspladsers datasikkerhed. Der er selvfølgelig enkelte nuancer.

Herunder at de it-professionelle generelt i den private sektor vurderer hackertruslen fra fremmede stater, terrororganisationer, organiseret kriminalitet, politiske/ideologiske hackere til at være lavere for deres virksomheder end de it-professionelle i den offentlige sektor gør. Hvorvidt det skyldes, at truslen er lavere eller de private virksomheder har et bedre værn, siger resultaterne ikke noget om.

Tabel 3. Hvordan vurderer du hackertruslen mod din egen organisations/virksomheds datasikkerhed fra?
Fordelt på privat og offentlig sektor. Pct.

	Lav		Middel		Høj		Ved ikke		I alt
	Privat	Off.	Privat	Off.	Privat	Off.	Privat	Off.	
Fremmede stater	36 %	27 %	23 %	25 %	28 %	32 %	13 %	16 %	100 %
Terrororganisationer	53 %	39 %	17 %	26 %	15 %	16 %	15 %	19 %	100 %
Organiseret kriminalitet	20 %	18 %	34 %	32 %	34 %	30 %	12 %	19 %	100 %
Politiske/ideologiske hackere	40 %	24 %	29 %	42 %	17 %	20 %	14 %	14 %	100 %
Interne trusler	41 %	41 %	36 %	32 %	9 %	14 %	14 %	13 %	100 %
Andet	16 %	17 %	18 %	19 %	10 %	3 %	56 %	60 %	100 %

Kilde: IDA Analyse (2019): Hackertruslen mod Danmark – analyse blandt IDAs it-professionelle
Note: n_privat = 374 n_offentlig = 93

Interne trusler vurderes fra begge sektorer til at være overvejende lav eller middel, idet kun 9 og 14 pct. fra hhv. privat og offentlig sektor vurderer denne til at være høj. Dette kan indikere, at enten værn mod interne trusler er relativt robust og/eller at organisationens/virksomhedens kompetenceniveau i forhold til cybersikkerhed er på et sådant niveau, at menneskelige, utilsigtede handlinger udgør et minimum.

55 pct.: Hackertruslen fra fremmede stater mod Danmarks infrastruktur er høj

Danmarks infrastruktur er en central del af det danske samfund, og uden fx velfungerende energi- og vandforsyning får "hjulene vanskeligt ved at køre rundt". I takt med den danske infrastruktur er blevet mere og mere digitaliseret, er hackertruslen selvsagt også kun blevet større.

Ifølge IDAs it-professionelle er hackertruslen mod Danmarks infrastruktur størst fra fremmede stater. *Jf. tabel 4* svarer 55 pct., at truslen herfra er høj. 40 pct. mener, at truslen fra terrororganisationer er høj. Hver tredje mener, at den er høj fra organiseret kriminalitet. De færreste mener, at hackertruslen fra de listede muligheder mod Danmarks infrastruktur er lav.

Tabel 4. Hvordan vurderer du hackertruslen mod Danmarks infrastruktur (fx energi- og vandforsyning) fra?

Alle svar. Pct.

	Lav	Middel	Høj	Ved ikke	I alt
Fremmede stater	8 %	25 %	55 %	12 %	100 %
Terrororganisationer	13 %	34 %	40 %	13 %	100 %
Organiseret kriminalitet	17 %	38 %	33 %	13 %	100 %
Politiske/ideologiske hackere	21 %	41 %	25 %	13 %	100 %
Andet	12 %	19 %	13 %	56 %	100 %

Kilde: IDA Analyse (2019): Hackertruslen mod Danmark – analyse blandt IDAs it-professionelle
Note: n = 461

Fordeles de it-professionelle i hhv. privat og offentlig sektor, er de langt overvejende enige i vurderingen af truslerne fra de listede muligheder, hvorfor en selvstændig tabel herover ikke vurderes at være interessant at afrapportere.

52 pct.: Hackertruslen fra fremmede stater mod offentlige institutioner er høj

Den offentlige sektor i Danmark er en af de mest digitaliserede i verden. De fællesoffentlige digitaliseringsstrategier har i stort omfang ageret løftestang for digitalisering af såvel staten, kommunerne og regionerne. Det giver den offentlige sektor en masse muligheder, men det stiller også en masse krav til særligt sikkerheden og forsvaret mod hackere.

Tabel 5. Hvordan vurderer du hackertruslen mod data i Danmarks offentlige institutioner (fx kørekortsregistret, Sundhedsplatformen, mv) fra?

	Lav	Middel	Høj	Ved ikke	I alt
Fremmede stater	9 %	28 %	52 %	11 %	100 %
Terrororganisationer	21 %	35 %	32 %	12 %	100 %
Organiseret kriminalitet	8 %	33 %	48 %	11 %	100 %
Politiske/ideologiske hackere	17 %	39 %	32 %	12 %	100 %
Andet	12 %	18 %	14 %	55 %	100 %

Kilde: IDA Analyse (2019): Hackertruslen mod Danmark – analyse blandt IDAs it-professionelle
Note: n = 461

Tabel 5 viser, at ca. halvdelen af IDAs it-professionelle vurderer, at hackertruslen fra fremmede stater og fra organiseret kriminalitet mod Danmarks offentlige institutioner er høj. Knap hver

10. mener, at truslen herfra er lav. Hver tredje vurderer, at truslen også er høj fra terrororganisationer og politiske/ideologiske hackere. Dette billede går igen, når de it-professionelle inddeles i hhv. privat og offentlig sektor. Resultaterne understøtter den tidligere nævnte pointe om, at digitalisering forpligter. Truslen fra ondsindede kræfter vurderes generelt at være stor mod data i de danske offentlige institutioner, hvorfor den offentlige sektor har en tvungen opgave i forhold til i) at topprioritere cyber- og – informationssikkerhed og ii) at sikre et højt kompetenceniveau, herunder gøre sig umage for at tiltrække dygtige it-sikkerhedsspecialister og efteruddanne den eksisterende medarbejderstab.

Tabel 6 viser, hvilke it-kompetencer de to sektorer har vanskeligt ved at rekruttere. Her ses det, at ca. hver tredje it-professionel ansat i den offentlige sektor mener, at de har vanskeligt ved at rekruttere it-kompetencer indenfor sikkerhed/security. IDA betragter dette som en kæmpe udfordring, idet vi uden de rette kompetencer på holdet, får meget vanskeligt ved at holde hackere i skak og dermed beskytte alle de data, som de offentlige institutioner ligger inde med om os alle sammen.

Tabel 6. Hvilke it-kompetencer er det vanskeligt at rekruttere? Pct.

	Privat	Offentlig
Systemudvikling/Arkitektur	47 %	45 %
Design og kommunikation	8 %	7 %
Test/Kvalitet	15 %	9 %
Programmering	45 %	30 %
Brugerunderstøttelse	3 %	9 %
Drift host/slutbrugerudstyr/netværk	13 %	19 %
Sikkerhed/security	22 %	31 %
It og forretningsprocesser	18 %	15 %
It-ledelse/it-projektledelse	17 %	17 %
Undervisning i it	3 %	16 %
Andet	15 %	28 %

Kilde: IDA Analyse (2019): Hackertruslen mod Danmark – analyse blandt IDAs it-professionelle
Note: n_privat = 346 n_offentlig = 86.

Hvem skal håndtere truslerne?

Analysen har indtil videre belyst, at Danmark på flere områder har en hackertrussel hængende over hovedet. Når hackertruslen er en uundgåelig bagside af digitaliseringsmedaljen, er det væsentligt at drøfte, hvilken instans der håndtere denne udfordring bedst.

FE vurderes til at være de bedste til at håndtere hackertruslen mod Danmark

Ifølge IDAs it-professionelle vurderes Forsvarets Efterretningstjeneste (FE), og herunder Center for Cybersikkerhed, at være bedst til at håndtere hackertruslerne. Jf. *tabel 7* mener 88 pct., at FE er den rette aktør. Herefter følger Politiets Efterretningstjeneste (PET) med 73 pct., Datatilsynet med 52 pct. og civile aktører med opbakning fra 50 pct.

Tabel 7. Hvem vurderer du, er de rette aktører til at håndtere truslerne?

	Antal	Procent
Forsvarets Efterretningstjeneste (FE)	338	88 %
Politiets Efterretningstjenester (PET)	335	73 %
Datatilsynet	236	52 %
Civile aktører	229	50 %
Andet	58	13 %

Kilde: IDA Analyse (2019): Hackertruslen mod Danmark – analyse blandt IDAs it-professionelle
Note: n = 457
Note: Respondenterne havde mulighed for at vælge flere svar, hvorfor det ikke summerer til 100 pct.

65 pct.: Ja tak til et nationalt, uafhængigt, rådgivende cybersikkerhedsorgan

I Danmark er ansvaret for Danmarks cybersikkerhed fragmenteret. Center for Cybersikkerhed under Forsvarsministeriet varetager noget af opgaven. PET under Justitsministeriet gør noget andet. Datatilsynet noget tredje. Og de private virksomheder og borgerne/forbrugerne gør, hvad de kan for at passe på sig selv.

Center for Cybersikkerhed har nogle samarbejds- og koordineringsorganer på tværs af ministerier og private virksomheder, men disse er langt fra tilstrækkelige. For det første mødes disse slet ikke hyppigt nok og for det andet, har de ikke et reelt mandat og derfor heller nogen nævneværdig gennemslagskraft.

I Holland har man erkendt, at cybersikkerhedstruslen ikke skal bekæmpes i siloer. Den skal bekæmpes i et forpligtende samarbejde mellem offentlige myndigheder, private virksomheder og forskningsverden. Derfor har man etableret det såkaldte Cyber Security Raad, som er et nationalt, uafhængigt rådgivende cybersikkerhedsorgan, der bistår både den hollandske regering og de hollandske private virksomheder. Rådet består af i alt 18 "high-rank" personer, herunder 7 fra den offentlige sektor, 7 fra den private og 4 fra forskningsverden. De mødes ugentligt for blandt andet at i) yde strategisk rådgivning til regeringen og de private virksomheder, ii) monitorere trends og nye teknologier mhp. at belyse deres potentiale ift. at reducere cybersikkerhedstruslen og iii) initiere og accelerere forskellige initiativer i både Holland og EU, som kan forbedre Hollands cybersikkerhedsforsvar.

IDA har med udgangspunkt i den hollandske model spurgt sine it-professionelle medlemmer om deres holdning til et tilsvarende organ her i Danmark. Resultaterne fremgår af *tabel 8*. her ses det, at 65 pct. mener, at et sådant organ vil være en god ide. 16 pct. mener, at ressourcerne

bør centreres hos FE og PET og 6 pct., at ressourcerne skal bruges på at styrke Datatilsynet. Flertallet er således for en model, som den de med succes har etableret i Holland.

Tabel 8. Hvad tænker du om det?
Indledende spørgsmålstekst: "Der er forslag om at oprette et råd baseret på civile aktører, offentlige myndigheder, forskere og virksomheder, som har til opgave at overvåge cyberangreb mod danske virksomheder og offentlige institutioner og advare og rådgive."

	Antal	Procent
Ja, det vil være en god ide	296	65 %
Nej, ressourcerne bør centreres hos FE og PET	74	16 %
Nej, ressourcerne skal bruges på at styrke Datatilsynet	29	6 %
Ved ikke	58	13 %
I alt	457	100 %

Kilde: IDA Analyse (2019): Hackertruslen mod Danmark – analyse blandt IDAs it-professionelle

De 65 pct. it-professionelle, som synes, at et nationalt, uafhængigt, rådgivende cybersikkerhedsorgan er en god ide, blev også bedt om at tage stilling til, hvilke kompetencer og ansvarsområder organet skal have. Svaret fremgår af *tabel 9*.

Her ses det, at de it-professionelle generelt er forholdsvis positive overfor de listede muligheder. Mest begejstret (86 pct.) er de dog overfor, at organet skal kunne rådgive virksomheder og myndigheder i forskellige sektorer. Og mindst begejstret (61 pct.) er de overfor, at organet skal være let tilgængeligt. De it-professionelle har også mulighed for at svare "andet", men kun 8 pct. benytter sig af denne mulighed, hvilket indikerer, at de listede muligheder kan betragtes som dækkende for, hvad sådan et organ skal kunne.

Tabel 9. En sådan organisation skal:

	Antal	Procent
Rådgive virksomheder og myndigheder i forskellige sektorer	256	86 %
Hurtigt sende advarsler, når der er opdaget angreb	242	82 %
Kunne melde ud og advare, men behandle indmeldte hændelser fortroligt	225	76 %
Lave undersøgelser af, hvor godt sikkerhedsniveauet er	215	73 %
Være let tilgængelig	180	61 %
Andet	24	8 %

Kilde: IDA Analyse (2019): Hackertruslen mod Danmark – analyse blandt IDAs it-professionelle
Note: n = 296 (dem der har svaret "ja, det vil være en god ide" på forrige spørgsmål)
Note: Respondenterne havde mulighed for at vælge flere svar, hvorfor det ikke summerer til 100 pct.

Metode og repræsentativitet

Metode

Undersøgelsen er gennemført blandt alle erhvervsaktive medlemmer af IDAs fagtekniske selskab IDA IT. 4.395 medlemmer af IDA IT blev inviteret til at deltage i undersøgelsen. Heraf har 672 svaret helt eller delvist på spørgeskemaet; svarende til en svarprocent på 15,3 pct.

Undersøgelsen er foretaget i perioden 1. til den 14. november 2018.

Repræsentativitet

Tabel 10. Køn (pct.)

	Medlemmer af IDA IT	Respondenter
Mand	90 %	92 %
Kvinde	10 %	8 %
Total	100 %	100 %

Kilde: IDA Analyse (2019): Hackertruslen mod Danmark – analyse blandt IDAs it-professionelle

Tabel 11. Alder (pct.)

	Medlemmer af IDA IT	Respondenter
Under 25 år	0 %	0 %
25-29 år	9 %	7 %
30-34 år	6 %	6 %
35-39 år	10 %	13 %
40-44 år	11 %	10 %
45-49 år	15 %	13 %
50-54 år	20 %	21 %
55-59 år	16 %	16 %
60-64 år	10 %	10 %
65 år eller ældre	3 %	4 %
Total	100 %	100 %

Kilde: IDA Analyse (2019): Hackertruslen mod Danmark – analyse blandt IDAs it-professionelle

Tabel 12. Ledelse (pct.)

	Medlemmer af IDA IT	Respondenter
Intet ledelsesansvar	72 %	73 %
Leder af ledere	2 %	2 %
Leder af medarbejdere	9 %	8 %

Projektleder	8 %	9 %
Selvstændig	6 %	6 %
Topchef	2 %	2 %
Total	100 %	100 %

Kilde: IDA Analyse (2019): Hackertruslen mod Danmark – analyse blandt IDAs it-professionelle

Tabel 13. Arbejdssektor (pct.)

	Medlemmer af IDA IT	Respondenter
Kommune	2 %	2 %
Privat	84 %	80 %
Region	2 %	3 %
Stat	12 %	15 %
Total	100 %	100 %

Kilde: IDA Analyse (2019): Hackertruslen mod Danmark – analyse blandt IDAs it-professionelle