ANALYSENOTAT

It-kriminalitet mod danske virksomheder vokser

AF CHEFKONSULENT MALTHE MUNKØE OG CHEF FOR DIGITALISERING JANUS SANDSGAARD

Cybersikkerhed er kommet højt op på dagsordenen i erhvervslivet og i den politiske verden. Konsekvenserne af it-kriminalitet kan være lammende både for den enkelte berørte virksomhed og for store dele af erhvervslivet og samfundets infrastruktur generelt, så som hospitaler, lufthavne og forsyning, som vi eksempelvis så det med "WannaCry"-angrebet tidligere på året.

Mange danske virksomheder oplever at truslerne, de står over for, er blevet større, mere sofistikerede, og flertallet forventer at denne udvikling vil fortsætte. Phishing og malware, hacking, CEO-fraud (hvor virksomhedens franarres penge ved at en kriminelle giver sig ud for at være direktøren der beder om en hurtig pengeoverførsel) og andre typer såkaldte cyberangreb er desværre noget, som i stigende grad truer rigtig mange virksomheder.

Dansk Erhverv har i en undersøgelse blandt vores medlemmer kortlagt omfanget af problemet, og set nærmere på de centrale udviklingstendenser. Blandt andet konstaterer vi, at:

- Danske virksomheder står over for en lang række "cybertrusler", fra phishing og malware til hacking, ransomware og CEO fraud. 73 pct. er blevet ramt eller forsøgt ramt af en eller flere typer "cyberangreb" – 28 pct. af et "succesfuldt" angreb/trussel, i den forstand at bagmændene opnåede, hvad de ville.
- Udfordringerne med it-kriminalitet rettet mod danske virksomheder er voksende: 48 pct. af virksomhederne er mere bekymrede i dag end for et par år siden, 55 pct. oplever at angrebene er blevet mere sofistikerede, og 68 pct. vurderer at truslen mod dem alt i alt er blevet større.
- 2 ud af 3 virksomheder mener det er sandsynligt, at de vil blive udsat for et angreb i 2018 – og ¼ virksomheder vurderer ligefrem, at det er sandsynligt at de bliver ramt af et succesfuldt angreb/trussel, hvor gerningsmændene får held med deres forehavende.
- Omkring halvdelen af virksomhederne i undersøgelsen har øget deres investeringer i cyber-sikkerhed, og en tilsvarende andel forventer at gøre det fremadrettet.
- Dette trusselsbillede nødvendiggør en række politiske tiltag, der sikrer erhvervsliv og samfundsliv bedre mod forskellige former for kriminalitet og cyberangreb.

Truslen fra cyberangreb fylder mere i danske virksomheder i dag, end for 2-3 år siden. Dette ses på baggrund af andelen af virksomheder, der vil øge deres ressourcer på it-sikkerhedsinvesteringer samt den generelle bekymring blandt virksomhederne.

Flertallet af virksomhederne ramt af cyberangreb de seneste år

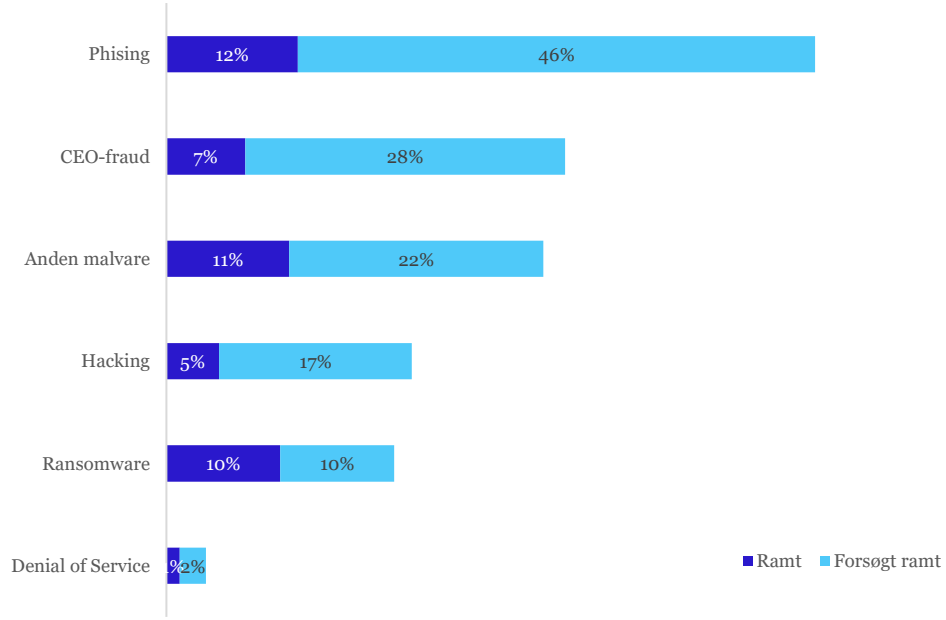
Ser man først detaljeret på, hvor udbredte de forskellige former for cybercrime er, ligger phishing og malware højt. Forsøg på CEO-fraud lader dog også til at være måske overraskende hyppigt forekommende, ligesom hacking udefra er noget knap hver femte virksomhed har oplevet de seneste par år.

Alt i alt er trusselsbilledet for de fleste danske virksomheder bredt, og spænder fra forskellige forsøg på at snyde medarbejdere via CEO-fraud og diverse malware- og phishing-mails til egentlige hackingangreb. Kun denial of service-angreb, der kan lægge en hjemmeside ned, er sjældne; hvilket måske kan ses i lyset af, at det er en form for cyber-kriminalitet, man ikke som bagmand tjener penge på.

Ser man samlet på det er det i alt 73 pct. af virksomhederne, der er blevet ramt eller forsøgt ramt af en eller flere af de forskellige viste typer cyberangreb – og 28 pct. af virksomhederne har været ude for et succesfuldt angreb, hvor det eksempelvis er lykkedesat en mail med malware er blev åbnet, hackerne fik adgang til systemet etc. Selvom de negative konsekvenser for firmaet kan variere afhængig af typen af angreb er det tydeligt, at risikoen er betydelig og at man mange steder har oplevet at sikkerheden ikke har været tilstrækkelig.

Figur 1

Er din virksomhed blevet ramt eller forsøgt ramt, af forskellige type cyberangreb de seneste 2-3 år, pct.



Phishing er mest udbredt, men også CEO-fraud, hacking og ransomware-angreb er noget, mange danske virksomheder desværre stifter bekendtskab med

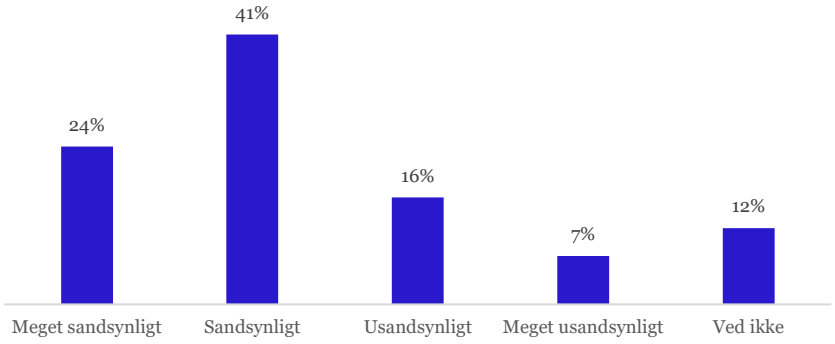
Kilde: Dansk Erhverv november 2017, n=259[i]

2 af 3 virksomheder forventer at blive ramt af et cyberangreb i 2018

Sammenlagt 65 pct. af de adspurgte virksomheder, mener at det er sandsynligt eller meget sandsynligt, at de vil blive udsat for mindst et cyberangreb i 2018. 23 pct. mener at det er usandsynligt eller meget usandsynligt.

Figur 2

Hvor sandsynligt tror du det er, at din virksomhed bliver udsat for et eller flere forsøg på cyberangreb i 2018?



2 ud af 3 virksomheder finder det sandsynligt eller meget sandsynligt, at de vil blive ramt af et cyberangreb i 2018

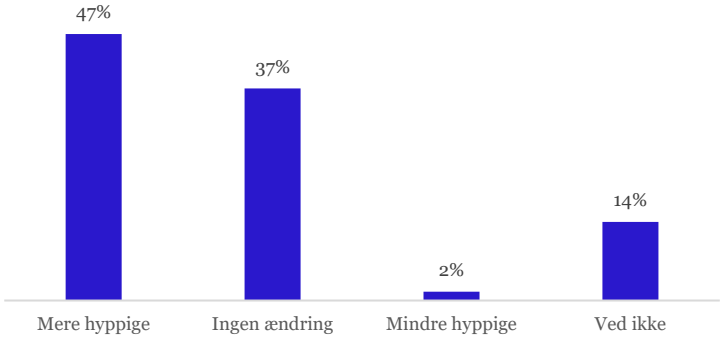
Kilde: Dansk Erhverv november 2017, n=259

Hyppigere og mere sofistikerede angreb

Cyberangrebene, som danske virksomheder udsættes for, bliver mere hyppige og mere sofistikerede, lyder den generelle vurdering. Knap halvdelen oplever således, at cyberangrebene mod dem er blevet mere hyppige, og stort set ingen har oplevet det modsatte. 55 pct. af virksomhederne angiver, at cyberangrebene generelt er blevet mere sofistikerede, og næsten ingen oplever at de er blevet mindre sofistikerede (jf. figur 4 nedenfor).

Figur 3

Oplever I at cyberangreb generelt er blevet mere hyppige eller mindre hyppige de seneste to år?

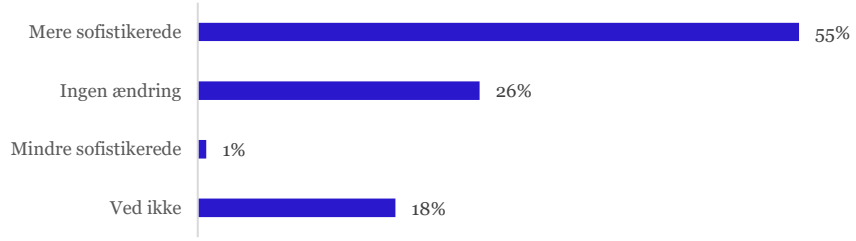


Næsten halvdelen af virksomhederne, 47%, oplever at cyber angreb sker hyppigere

Kilde: Dansk Erhverv november 2017, n=259

Figur 4

Oplever I at cyberangreb generelt er blevet mere sofistikerede (dvs. at personerne bag er blevet dygtigere) eller mindre sofistikerede de seneste to år?



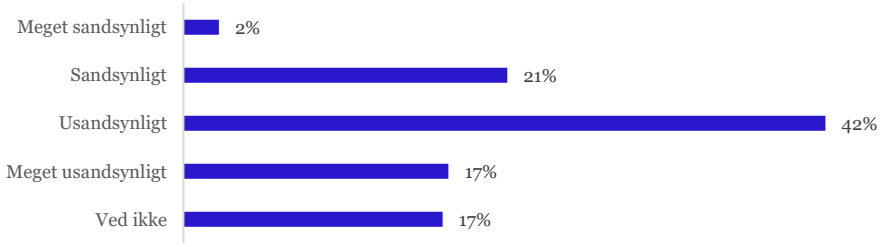
Kilde: Dansk Erhverv november 2017, n=259

¼ virksomheder regner med at blive ramt af et succesfuldt cyberangreb

Mange virksomheder oplever trusler næsten dagligt, når medarbejderne spammes til af dubiøse mails med malware, eller når hackere sætter sigtekornet på virksomheden. Men det er et "wake-up call" at hver fjerde virksomhed ligefrem regner med, at de i 2018 vil blive ramt af et succesfuldt cyberangreb, forstået sådan at bagmændene får held med det, de gerne vil opnår. Selvom truslerne selvfølgelig varierer meget i forhold til, hvor alvorlige følgerne vil være for virksomheden, er det et meget iøjenfaldende resultat, at en fjerdedel af erhvervslivet altså ligefrem regner med, at de vil opleve en eller anden form for skade på grund af it-kriminalitet i det kommende år.

Figur 5

Hvor sandsynligt tror du det er, at din virksomhed bliver udsat for et eller flere succesfulde cyberangreb i 2018 (dvs. et, hvor personerne bag har held til at opnå det de gerne vil, fx få adgang til jeres data)?



23% af virksomhederne finder det sandsynligt eller meget sandsynligt, at de ville blive succesfuldt ramt af et cyberangreb i 2018

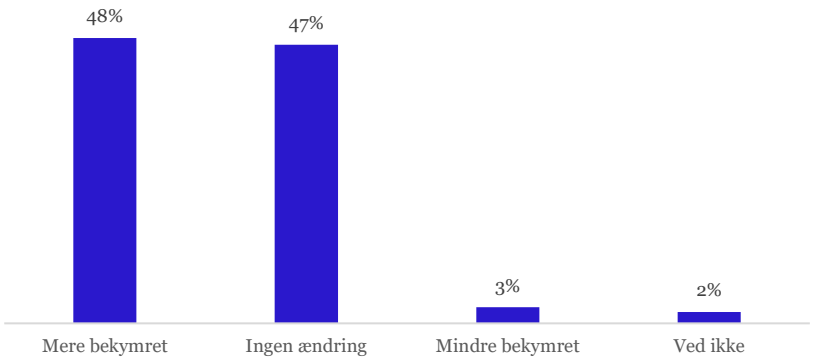
Kilde: Dansk Erhverv november 2017, n=259

Forventer mere alvorligt trusselsbillede fremover

Fremadrettet vurderer mange virksomheder, at cyberangreb vil blive et større problem. Mange er mere bekymrede i dag end for to år siden, og 68 pct. oplever, at truslen er blevet større (jf. figur 6 og figur 7).

Figur 6

Er du mere eller mindre bekymret i dag end for to år siden over risikoen for cyberangreb mod din virksomhed?

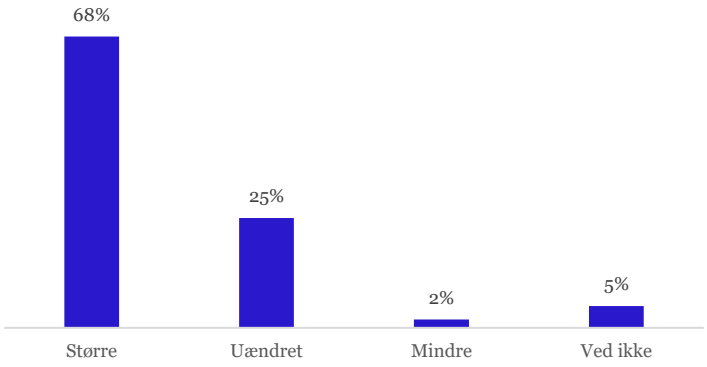


Næsten halvdelen af virksomhederne, 48%, er mere bekymrede for cyberangreb i dag end for 2 år siden

Kilde: Dansk Erhverv november 2017, n=259

Figur 7

Når du ser alt i alt på det, vurderer du så, at truslen fra cyberangreb er større eller mindre i dag end for to år siden?



2 ud af 3 virksomheder vurderer, at truslen fra cybercrime er større i dag end for 2 år siden.

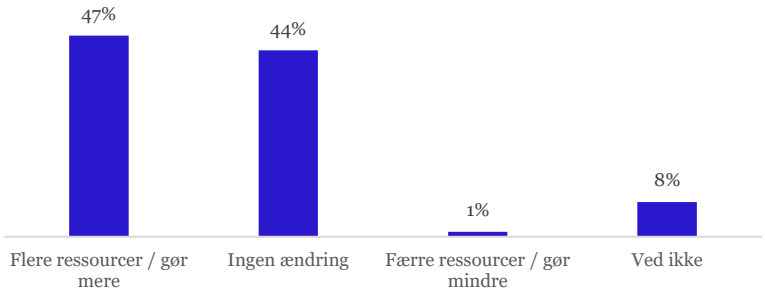
Kilde: Dansk Erhverv november 2017, n=259

Mange investerer mere – men ikke alle er med

Godt halvdelen af virksomhederne bruger flere ressourcer i dag end for to år siden på cybersikkerhed. Meget få bruger færre ressourcer. Alt i alt er der altså ingen tvivl om, at man mange steder – men altså omvendt langt fra alle steder – i erhvervslivet har fået et øget fokus på området.

Figur 8

Når du ser på jeres it-investeringer og it-medarbejdernes tidsforbrug osv., bruger I så flere eller færre ressourcer i dag end for to år siden på at beskytte jer mod cyberangreb?



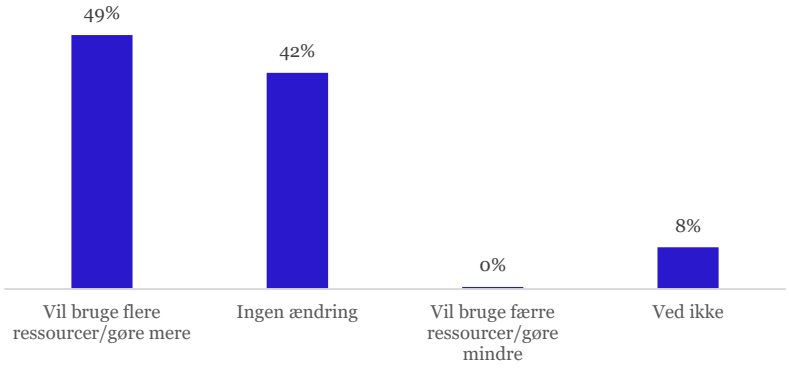
Kilde: Dansk Erhverv november 2017, n=259

Næsten halvdelen af virksomhederne, 47%, bruger i dag flere ressourcer på beskyttelse mod cyberangreb end for 2 år siden

Tilsvarende er det halvdelen som fremadrettet at bruge flere ressourcer på cybersikkerhed.

Figur 9

Når du ser på de kommende år, vurderer du så at din virksomhed vil bruge flere eller færre ressourcer for at beskytte jer mod cyberangreb end i dag?



Kilde: Dansk Erhverv november 2017, n=259

Næsten halvdelen af virksomheder, vurderer at de i de kommende år vil bruge flere ressourcer/gøre mere for at beskytte sig mod cyberangreb. Ingen forventer at bruge færre ressourcer/gøre mindre

Behov for politiske initiativer for bedre cybersikkerhed

Som følge af den voldsomme vækst i antallet og omfanget af trusler er der behov for stor politisk bevågenhed om cybersikkerhedsområdet på nationalt plan og i EU-regi.

På europæisk plan er NIS-direktivet (Directive on security of Network and Information Systems) blevet vedtaget og trådte i kraft i august 2016, med frist for den nationale implementering den 9. maj 2018. Direktivet vil blandt andet betyde, at der skal etableres en positivliste over operatører af "væsentlige tjenester", som har underretningspligt ved sikkerhedshændelser og forpligtes til at sikre en robust cyber-infrastruktur. Det er centralt at positivlisten fastlægges med en fornuftig afvejning imellem behovet for at sikre en tilstrækkelig beskyttelse af central infrastruktur og de omkostninger, de forøgede krav kan få for erhvervslivet.

Kommissionen foreslår et EU Cybersecurity Agency, der skal sikre stærkere europæiske koordinering mellem også EU og NATO. Arbejdet bygger videre på det hidtidige European Agency for Network and Information Security (ENISA), men med øget bevilling og permanent mandat. Det støtter Dansk Erhverv varmt. Internettet er per definition grænseoverskridende. Der er tale om internationale problemer, der kræver internationale løsninger.

Skulle vi savne noget er det samarbejde, der rækker ud over EU. Her har Dansk Erhverv tidligere talt for en global digital Geneve-konvention[ii], der skal beskytte civil infrastruktur, hvor lande og virksomheder tiltræder en række spilleregler om deling af viden om sårbarheder i it-systemer og om ikke at angribe civil infrastruktur. Eksempelvis vil det være hensigtsmæssigt at forsøge at skabe international accept af, at det ikke er acceptabelt at gennemføre cyberangreb mod hospitalsinfrastruktur, ligesom det at angribe hospitaler ikke er tilladt efter den normale krigs love. Mere generelt er det vigtigt at EU forsøger at skabe enighed i FN, trods de vanskeligheder det indtil nu har været forbundet med, omkring fælles spilleregler på området.

Samtidig er det i national sammenhæng hensigtsmæssigt at se på, hvilken forstærket rolle de danske myndigheder kan spille i forhold til cybersikkerhed. Aktuelt tilskrives Forsvarets Center for Cybersikkerhed en stor rolle, samtidig med at Dansk Erhverv har talt for en national strategi for cyber- informationssikkerhed[iii] der omfatter alle myndighedsniveauer. Derfor hilser i det velkommen at regeringen afsætter 100 mio. kr. til en styrket indsats med deltagelse af flere myndigheder også private aktører. Den kommende cyber- og informationssikkerhedsstrategien forankres i Finansministeriet, vil gælde i perioden 2018-2020, og forankres i en tværministeriel arbejdsgruppe med repræsentanter for 13 ministerier. Regeringen forventer at fremlægge strategien i begyndelsen af det nye år. Det vil være hensigtsmæssigt at erhvervslivet i højere grad også får adgang til relevante informationer om sikkerhedstrusler og hændelser.

At informationssikkerhed er et område i hastig bevægelse ses også af, at EU sætter også fokus på "Tingenes internet" (Internet of Things, IoT). Udviklingen af IoT handler om,

at alt fra husholdningsapparater til legetøj flytter på internettet. Der er en risiko for, at dette vil skabe nye sårbarheder, som it-kriminelle kan udnytte. Dansk Erhverv hilser det velkomment, at Kommissionen har fokus på at afsøge muligheden for at øge cybersikkerheden i EU ved hjælp af certificerings- og standardiseringsordninger, og i øvrigt sætter fokus på at forbedre forbrugernes og virksomhedernes cyberhygiejne, dvs. altså uddannelse i, hvordan man omgås forbundne enheder og tager basale forholdsregler.

Fakta om analysens datagrundlag

Analysen er baseret på data indsamlet via en medlemsundersøgelse gennemført blandt et tilfældigt udvalgt udsnit af Dansk Erhvervs medlemmer. I alt er indsamlet 259 besvarelser i november 2017. Undersøgelsen vurderes at være bredt dækkende for Dansk Erhvervs medlemmer, som udgør et bredt udsnit af det danske erhvervsliv, med særlig vægt på servicesektoren, som udgør ca. 70 pct. af alle private beskæftigede.

Med survey-analyser af denne karakter kan der være en risiko for, at der sker et systematisk frafald af virksomheder, der ikke oplever problemer og derfor ikke interesserer sig for emnet omkring cybersikkerhed, der derfor undlader at svare. I kontakten til vores medlemmer har vi gjort alt for at opfordre dem til at svare også selvom de ikke oplever aktuelle udfordringer. Den anvendte stikprøve adskiller sig ikke markant fra hvad der kan forventes ved et tilfældigt udsnit af medlemspopulationen eller de stikprøver, Dansk Erhverv typisk får. Derfor vurderes resultaterne alt i alt at være generelt dækkende.

◥ OM DETTE NOTAT

"Cyber-truslen mod danske virksomheder vokser" er Dansk Erhvervs analysenotat nummer 66 i 2017. Redaktionen er afsluttet den 5. december 2017.

◥ OM DANSK ERHVERVS ANALYSENOTATER

Dansk Erhverv udarbejder løbende analyser, som samles i analysenotater. Ambitionen er at udgøre et kvalificeret og anvendeligt beslutningsgrundlag i forhold til væsentlige, aktuelle udfordringer på alle områder, som har betydning for dansk erhvervsliv og den samfundsøkonomiske udvikling. Det er tilladt at citere fra Dansk Erhvervs analysenotater med tydelig henvisning til Dansk Erhverv.

◥ KVALITETSSIKRING

Troværdigheden af tal og analyser fra Dansk Erhverv er afgørende. Dansk Erhverv gennemfører egne spørgeskemaundersøgelser i overensstemmelse med de internationalt anerkendte guidelines i ICC/ESOMAR, og alle analyser og beregninger gennemgår en kvalitetssikring.

◥ KONTAKT

Henvendelser angående analysen kan ske til chefkonsulent Malthe Munkøe på mmm@danskerhverv.dk eller tlf. 3374 6510.

Henvendelser angående digitalisering, datasikkerhed og cybertrusler kan ske til fagchef Janus Sandsgaard på jsa@danskerhverv.dk eller tlf. 3374 6239.

◥ NOTER

[i] Svarmulighederne var:
Ja, vi er desværre blevet ramt af denne type cyber-kriminalitet
Vi er blevet forsøgt angrebet, men det lykkedes ikke for dem
Nej, har ikke oplevet det
Ved ikke

[ii] Se fx Politiken den 29. juni 2017: "NSA har på ny medansvar for ødelæggende angreb: Erhvervslivet kræver digital våbenkontrol" http://politiken.dk/udland/art6014269/Erhvervslivet-kr%C3%A6ver-digital-v%C3%A5benkontrol

[iii] "Dansk Erhvervs digitale politik – vækst gennem digitalisering "(maj 2017) - http://www.danmarkdigitalt.dk/politik/sikkerhed/