AALBORG UNIVERSITET

CYBERSIKKERHED

I EN KONSTANT UDVIKLENDE DIGITAL VERDEN

Et speciale om hvordan revisorer sikrer sig, at virksomhederne lever op til de krav, der er til cybersikkerhed, så de sikkert kan agere i den digitale verden.

Rasmus Madsen Carlslund
Studienummer: 20155011

Speciale, maj 2020

Cand.merc.aud, Aalborg Universitet

Vejleder: Hans Henrik Berthing

Antal sider: 64 sider

Abstract

This master's thesis reflects upon the phenomenon cybersecurity, and the role of an auditor, in helping Danish companies securely navigating in the constantly changing digital world.

The methodological approach is the hermeneutic circle, and deals with the interpretation and understanding of social reality. Through the interpretation of several cybercrime studies, the thesis seeks to gain an understanding of cybercrime as well as to find cause and effect in the empirical data collected.

The thesis explains the standards that the auditor have at their disposal and how they are used in accordance to cybersecurity. Furthermore it explains 1) what cybercrime is, 2) what vulnerabilities the Cyber Security Committee believes there are, 3) what cyber security is in relation to PwC's Cybercrime Survey 2019, as well as 4) the challenges that the corona crisis brings in relation to cyber security and 5) what types of attacks that occur during the corona crisis.

The analysis looks into how the Danish companies are affected by cybercrime and how they are handling these attacks. The Danish companies are experiencing a rise of attacks, and the corona crisis only increases the pressure on the companies' cyber security. The thesis reflects upon the Financial crisis in 2008, and how it affected the IT-budgets in order to gain an understanding of the possible outcome of the corona crisis.

The discussion revolves around the following themes: 1) ISAE 3000, ISAE 3402 and ISRS 4400, 2) How auditors must constantly keep themselves updated, 3) The discrepancy between perceived reality and actual reality, 4) How smaller companies reduce IT budgets, while larger companies raise budgets, 5) If companies can rely on its controls if IT budgets are lowered, 6) How employees is the biggest threat, but also a strong defense, 7) The impact of the corona crisis, 8) The future of IT security, 9) A brief look back on the Financial crisis, 10) The future of the auditor, and 11) The national focus on cyber security

The thesis concludes that, cybersecurity is a constant race with time before the next major attack or crisis strikes, so it is better to act today, than to regret it tomorrow.

Key words: Cybersecurity, cybercrime and the role of the auditor

Rasmus Madsen Carlslund
Cand.merc.aud.
Den 31. maj 2020

Indholdsfortegnelse

Rasmus Madsen Carlslund
Cand.merc.aud.
Den 31. maj 2020

Indledning

> "*Digitaliseringen bidrager med meget godt til vores samfund. Men i ivrighed efter at blive endnu mere digitale bliver der også nogle gange truffet beslutninger, uden at sikkerheden er på plads.*"[1]

Sådan udtaler forsvarsminister, Trine Bramsen til CXO-magasinet i 2020. Hun understreger yderligere, at den digitale udvikling sker med så stor hastighed, at det kan være en udfordring for virksomhederne at følge med og samtidig have styr på IT-sikkerheden. Derfor mener hun, at det er et "kapløb med tiden"[2].

Ikke mindre end 51 % af de adspurgte virksomheder har i ifølge Cybercrime Survey 2019 indenfor de seneste fem år som minimum oplevet ét cyberangreb[3]. De økonomiske konsekvenser kan være vidtrækkende, og det kan koste op mod halve til hele milliarder for virksomhederne at blive ramt at ondsindede aktører. Derfor er det ikke underligt, at en stigende og rekordhøj andel af topchefer frygter cyberangreb [4].

Kernen i mange danske virksomheder er data, og derfor er data milliarder kroner værd, og brud på datasikkerheden kan derfor have fatale konsekvenser for mange virksomheder. Det understreger vigtigheden af professionel IT-sikkerhed og -kontroller, som revisorer rådgiver de danske virksomheder om.

Forsvarsminister Trine Bramsen udtaler, at mange private virksomheder holder det hemmeligt, når de er blevet angrebet af cyberkriminalitet. Hun mener, at årsagen kan være, at virksomhederne finder det pinligt, og at det er dårligt for virksomheden

[1] Bramsen, 2020
[2] Bramsen, 2020
[3] PwC, Cybercrime Survey 2019, 2019
[4] Mortensen, 2020

brandværdi[5]. Det betyder, at der kan være et stort skyggetal af cyberangreb, som man ikke kender til.

> "*Det svarer til, at politiet er nødt til at vide, at der har været et indbrud for at kunne fange forbryderne, der står bag*"[6],

udtaler Trine Bramsen og efterlyser en større åbenhed fra de danske virksomheder.

Qua den konstant foranderlige digitale udvikling er IT-sikkerhed og -kontroller en "never ending story". God IT-skik kræver kontintinuerlig opdatering af virksomhedens IT-sikkerhed og -kontroller[7].

Revisor har en række muligheder, som kan give virksomheder en vis sikkerhed både i deres egne cybersikkerhedskontroller ved brug af outsourcing leverandører og i forhold til, hvem de har samarbejde med.
Revisor er offentlighedens tillidsrepræsentant jf. Revisorloven §16, og derfor er der en høj grad af tillid over for de erklæringer, revisor kommer med. Derfor kan revisor være med til at bidrage til, at virksomheder handler og bevæger sig i den digitale verden på forsvarlig vis.

Det er ikke nyt, at revisorer beskæftiger sig med virksomhedernes IT-anvendelse. I 1989 udgav FSR den første vejledning omkring IT: "Revision i virksomheder som anvender EDB" (Revisionsvejledning nr. 14)[8]. Siden er der kommet mange forskellige standarder, krav og love til, som er med til at sikre, at virksomheder ikke bliver overrumplet på den digitale front. Af de helt store trusler man ser i dag er phishing og ransomware på vej tilbage, og især i krisetider ser ondsindede aktører muligheden for at få en bid af kagen[9].

[5] Bramsen, 2020
[6] Bramsen, 2020
[7] Berthing, Mogensen, Lind, Gotfredsen, Mikkelsen & Nielsen, 2011
[8] Mogensen, 2018
[9] PwC, Cybercrime Survey 2019, 2019

Det er vigtigt, at der er tillid til revisors arbejde. Ligeså spiller tilliden en stor og afgørende rolle i samarbejdet mellem virksomheder. Det er vigtigt, at der er tillid til at den anden part også har styr på IT-sikkerheden f.eks. i forhold til persondata. I PwC's webinar om cybersikkerhedsudfordringer i krisetider udtaler Natasha Lembke, partner og leder af PwC's Finance Effectiveness afdeling:

> "*Tillid er jo simpelthen altafgørende, når vi handler og arbejder sammen. Derfor skal jeg også have tillid til, at din sikkerhed (red. i en anden virksomhed) ligeså vel som at min sikkerhed (red. i min virksomhed) også skal være i orden.*"[10]

I min søgen efter mere information om emnet, er jeg blevet opmærksom på, at den danske presse har vist stor interesse for emnet i særdeleshed i forbindelse med corona-krisen f.eks. "Danske topchefer frygter hackere mere end nogensinde"[11].

Med corona-krisens indtog er hjemmearbejde pludseligt blevet hverdagen for mange danskere. Det betyder i mange tilfælde, at de manuelle kontroller er ekstra udsat. Det er for eksempel ikke lige så nemt at råbe ind til chefen: "*Michael, hvad er det for en mærkelig mail, du har sendt til mig*?" Det er for eksempel også adm. direktør i Købstædernes Forsikring, Anders Hestbechs pointe, når han skriver i et blogindlæg at:

> "*Vi (red. medarbejdere) er selv den største trussel.*"[12]

Anders Hestbech mener altså, at virksomhedernes største trussel ift. beskyttelse af data er deres medarbejdere[13]. IT-kriminelle er formodentlig kommet frem til samme konklusion, da man ser en stigning i antallet af cyberangreb fra IT-kriminelle[14].

[10] PwC webinar: Cybersecurity-udfordringer i krisetider, 2020
[11] Mortensen, 2020
[12] Hestbech, 2020
[13] Hestbech, 2020
[14] PwC webinar: Cybersecurity-udfordringer i krisetider, 2020

Virksomhederne møder i denne digitale krisetid helt nye udfordringer, hvad angår IT-sikkerhed pga. den stigende trussel fra IT-kriminelle og pga. af den nye situation, virksomhederne pludselig er i. Virksomhederne kan ikke fuldstændigt fjerne risikoen for cyberangreb, men de kan gøre meget for at minimere risikoen for angreb[15].

Ønsket bag dette speciale var helt fra start at lave et projekt, der har relevans ude "i virkeligheden" og ikke kun i den akademiske verden. Med corona-krisens indtog er specialets relevans blevet forstærket.

Med udgangspunkt i ovenstående indledning er specialets problemformulering som følger.

Problemformulering

Hvordan sikrer revisorer sig, at virksomhederne lever op til de krav, der er til cybersikkerhed, så de sikkert kan agere i den konstant udviklende digitale verden?

For at kunne besvare problemformuleringen vil relevante standarder blive gennemgået og diskuteret. Dertil er det også vigtigt at vide, hvordan det danske erhvervsliv generelt og specifikt forholder sig til cyberkriminalitet og cybersikkerhed. Derfor vil dette speciale også besvare nedenstående underspørgsmål:

- ➔ **Underspørgsmål 1:** Hvordan håndteres truslen om cyberkriminalitet blandt de danske virksomheder generelt?
- ➔ **Underspørgsmål 2:** Hvordan påvirker corona-krisen cyberkriminalitet og virksomhedernes IT-sikkerhed, og hvordan kan virksomhederne håndtere krisen?

[15] PwC webinar: Cybersecurity-udfordringer i krisetider, 2020

Underspørgsmål 1 besvares gennem analyse og diskussion af Cybercrime Survey 2019 udgivet af PwC[16].

Underspørgsmål 2 besvares i specialet gennem analyse og diskussion af:

1. COVID-19 CFO Pulse Survey[17]: Corona-krisens indflydelse på IT-sikkerhed, udarbejdet af PwC
2. Webinar: Cyber Security-udfordringer i krisetider[18], lavet af PwC.

Ydermere besvares underspørgsmål 2 også med en perspektivering til Gartner CIO Survey fra 2009[19], som handler om cybersikkerhed efter Finanskrisen.

[16] PwC, Cybercrime Survey 2019, 2019
[17] PwC, COVID-19 CFO Pulse Survey, 2020
[18] PwC, Cybersecurity-udfordringer i krisetider, 2020
[19] Gartner, 2009

Metode

Det følgende afsnit omhandler den metodiske tilgang til dette speciale. Formålet med afsnittet er at gøre processen transparent, så der ikke er nogen tvivl om, hvordan konklusionerne er fremkommet. Afsnittet svarer derfor på hvilken fremgangsmåde, der er benyttet og hvad begrundelsen er for valgene i processen.[20]

Projektet søger som bekendt at undersøge, hvordan revisorer sikrer sig, at virksomhederne lever op til de krav, der er til cybersikkerhed, så de sikkert kan agere i den konstant udviklende digitale verden.

Indledningsvist vil metodeafsnittet omhandle den filosofiske hermeneutik, som forklarer den videnskabelige grundforståelse, som er fundament for specialet.

Hermeneutik

Hermeneutik beskæftiger sig med fortolkning og forståelse af den sociale virkelighed [21]. Gennem fortolkning af flere cyberkriminalitets-undersøgelser ønsker specialet at opnå forståelse for cyberkriminalitet samt at finde årsager og sammenhænge i den indsamlede empiri. Jf. hermeneutikken findes der ikke en endegyldig viden[22] og den hermeneutiske tilgang er et opgør mod tanken om, at metode fører til sand viden[23].

Der er ikke kun én udlægning af fortolkningen af disse undersøgelser, men fortolkningen vil være forskelligt fra individ til individ. Det betyder, at fortolkeren, som i dette tilfælde er specialets forfatter, har stor betydning for specialets fortolkninger og dermed konklusioner.

[20] Rienecker & Stray Jørgensen, 2013
[21] Højbjerg, 2009
[22] Højbjerg, 2009
[23] Juul, 2012

Resultater af forskning er et produkt af det gensidige samspil mellem det fænomen, som undersøges og den, som undersøger fænomenet. Fortolkeren spiller derfor en central rolle i udarbejdelsen af dette speciale. Det skyldes, at fortolkeren ikke kan gå fuldstændig neutralt til fænomenet, da fortolkeren er påvirket af sin egen forståelseshorisont, som består af forforståelser og fordomme:

> "*Forståelseshorisonten er konstitueret af sprog, personlige erfaringer, tidslighed i form af fortid, fremtid og nutid samt af den historiske og kulturelle kontekst, som den enkelte er indlejret i. Det er den som sætter rammen om vores blik på verden og udfordrer vores tilgang til verden. Den er altså foranderlig og i konstant bevægelse.*"[24]

Det betyder, at jeg som forfatter af dette speciale har indflydelse på specialet gennem hele processen. Det har forfatteren af dette speciale en bevidsthed om, men med hermeneutik som metodiske tilgang accepteres det også, at det er uundgåeligt at være neutral.

Den hermeneutiske cirkel

Når man skal forstå noget, starter man ikke forfra. Vores fortolkning bygger ovenpå eksisterende forforståelse og fordomme. Den hermeneutiske cirkel handler om at forstå delene ud fra helheden og helheden ud fra delene.[25]

Det betyder, at fortolkeren ikke kan gå neutralt til et fænomen, men der er en vekselvirken mellem fænomenet og fortolkeren. Derfor kan det være svært at replikere dette speciale, da specialet er påvirket er min forforståelse og fordomme. Cyberkriminalitet er et menneskeskabt og levende fænomen, som er i konstant forandring, hvilket i særdeleshed er blevet tydeligt under corona-krisen.

[24] Højbjerg, 2009, s. 323
[25] Juul, 2012

En dynamisk specialeudvikling

I specialeprocessen har der været en flydende problemformulering, og derfor har projektets emne udviklet sig undervejs. Det har gjort plads til, at specialet har kunne inddrage corona-krisen i specialet, hvorfor specialet er blevet mere relevant desto længere, det er kommet i processen. Udviklingen omkring cyberkriminalitet og cybersikkerhed er blevet fulgt tæt i medierne.

Dataindsamling: Kvantitativ data

Dette projekt søger at analysere en stor mængde sekundær kvantitativ data fra flere forskellige undersøgelser. En præmis for kvantitativ dataanalyse er muligheden for at finde årsage og sammenhænge i den indsamlede data[26], hvilket også er målet i dette speciale. Fordelen ved den kvantitative analyse er, at den kan generalisere grundet den store mængde data[27].

Når specialet søger at finde årsag og sammenhæng kan det godt klinge af en mere naturvidenskabelig tilgang, hvilket ikke er situationen. Det mønster, som måske måtte vise sig i den indsamlede data, er stadig udtryk for forfatters fortolkning og er derfor ikke et neutralt udlæg af fænomenet. Jeg hverken kan eller bør frasige mig min egen fortolkning, da denne fortolkning er fremkommet på baggrund af en bachelor i Economics and Business Administration og snart to år på Revisions-uddannelsen. Det er relevante briller at kigge ud af, når data skal analyseres for at skabe et billede af hvordan cyberkriminalitetsverdenen hænger sammen.

Undervejs i specialet har omdrejningspunktet kontinuerligt været IT-ledelse, men det er et projekt i forandring. Da disse udvalgte undersøgelser blev fundet, blev cyberkriminalitet sat i fokus.

[26] Kuada, 2014
[27] Bryman, 2012

De udvalgte surveys er valgt til at afdække fænomenet, men de er også valgt på baggrund af deres høje troværdighed, som er videre uddybet under afsnittet om kildekritik.

En præmis for kvantitativ data er, at dataen er repræsentativ. Omvendt er præmissen også, at den kvantitative data ikke kan levere dybdegående og uddybende indsigt i dataen[28]. For at kompensere for dette, var ønsket at foretage semistrukturerede interviews, som beskrevet i nedenstående afsnit.

Jeg kunne med høj sandsynlighed ikke selv have foretaget en undersøgelse af virksomhedernes IT-sikkerhed, hvorunder de svarer på, om de er blevet angrebet af cyberkriminelle. Det skyldes, som forsvarsminister Trine Bramsen udtaler at:

> *"Blandt private virksomheder er der stadig en stor tilbageholdenhed i forhold til at fortælle, når de har været udsat for angreb. De synes øjensynligt, at det er pinligt – eller også vil de bare ikke risikere, at det rygtes i markedet, at de har været offer for et angreb."*[29]

Det er altså et svært tilgængelig data, som PwC præsenterer i deres surveys.

Dataindsamling: Kvalitativ data

For at uddybe fænomenet cyberkriminalitet yderligere skulle kvalitative interviews have været udført. Formålet med at udføre semistrukturerede interviews med revisorer var at få en dybdegående forståelse af, hvordan revisorer sikrer sig, at virksomhederne lever op til de krav, der er til cybersikkerhed, så de sikkert kan agere i den konstant udviklende digitale verden. Grundet corona-krisen har det desværre ikke været muligt at indhente primær data i form af interviews med revisorer, da tilgængeligheden ikke har været til stede.

[28] Bryman, 2012
[29] Bramsen, 2020

Som beskrevet giver den kvantitative data en mere generel og bred beskrivelse og på den måde kompenserer den kvalitative og kvantitative data hinanden. Det semistrukturerede interview har jf. Kvale & Brinkmann[30] til formål at give forskeren et nuanceret indblik i den interviewedes syn på et bestemt emne for efterfølgende at kunne opnå forståelse gennem fortolkning.[31], hvorfor det var et ønske at udføre interviews med revisorer.

Det er dog lykkedes at komme omkring problematikken ved at stille spørgsmål til et webinar fra PwC omhandlende *Cyber Security i krisetid*[32]. Spørgsmål til eksperterne i et webinar kan ikke sidestilles med et egentligt interview, men det gav nogle nuancerede svar[33].

Kildekritik

Den store undersøgelse, Cybercrime Survey 2019[34], som leverer størstedelen af empirien til dette speciale, er produceret af PwC, men bakket op af store tillidsvækkende brancheorganisationer og firmaer. Specialet forholder sig kritisk til kilden, da PwC sælger IT-rådgivning. Det formodes, at undersøgelsen har en agenda, idet PwC formentligt ønsker at sælge flere af disse IT-revisionsydelser. Derfor taler undersøgelsen umiddelbart deres sag. Omvendt lever PwC også af, at deres kunder har stor tillid til dem. Derfor er sandsynlighed for at undersøgelsen ikke er troværdig og valid meget lille. Især opbakningen fra ISACA taler for, at undersøgelsen er fuldt ud troværdig, da ISACA er en højst pålidelig kilde.

[30] Kvale & Brinkmann, 2015
[31] Bryman, 2012
[32] PwC, Cybersecurity-udfordringer i krisetider, 2020
[33] Se bilag 1
[34] PwC, Cybercrime Survey 2019, 2019

Generelt er størstedelen af den anvendte empiri udarbejdet af PwC, men argumentationen i ovenstående gælder også for det andet empiri fra PwC[35] [36]. Dog bakkes de ikke op af store spillere i markedet.

Standarder og love vil ikke blive redegjort for i deres fulde længe, men vil blive redegjort ud fra deres relevans for specialet. Ved brug af Karnov Jura er validiteten af retskilden sikret.

[35] PwC, COVID-19 CFO Pulse Survey, 2020
[36] PwC, Cybersecurity-udfordringer i krisetider, 2020

Rasmus Madsen Carlslund
Cand.merc.aud.
Den 31. maj 2020

Redegørende afsnit

Formålet med dette afsnit er at redegøre for de udvalgte erklæringer, som revisor kan tage bruge i sit arbejde vedrørende cybersikkerhed. Af nedenstående tabel fremgår en oversigt over de standarder, der vil blive gennemgået i dette speciale.

Det redegørende afsnit vil slutteligt indeholde et afsnit, der forklarer, hvad cyberkriminalitet er.

Standard	Anvendelse i forhold til cybersikkerhed	Revisors konklusion
ISAE 3000[37]: Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger	Ved brug af ISAE 3000, vil der blive aftalt, hvilke handlinger revisor skal udføre og dette vil beskrives i erklæringen. Disse handlinger kan blive udført efter FSR's Cybersikkerhedsudvalgs skabelon efter hensigtsmæssige erklæringer.	Ved udførelsen af ISAE 3000 afgiver revisor en samlet konklusion ud fra de handlinger, der er beskrevet i erklæringen.
ISAE 3402[38]: Erklæringsopgaver med sikkerhed om kontroller hos en service leverandør	Ved brug af ISAE 3402 vil revisor udføre en række test på kontrolområder, kontrolaktiviteter og danne sig et overblik over hele virksomhedens system. Revisor skal derfor også danne sig et overblik over hvilke dele af IT-funktionerne, der ligger hos outsourcing leverandøren og hvilke	Ved udførelsen af ISAE 3402 afgiver revisor en konklusion ud fra de kontroller, som revisor har gennemgået i sin udførelse af erklæringen.

[37] ISAE 3000
[38] ISAE 3402

	kontroller, der er tilbage i virksomheden.	
ISRS 4400[39]: Aftalte arbejdshandlinger vedrørende regnskabsmæssige oplysninger og yderligere krav ifølge dansk revisorlovgivning	Ved brug af ISRS 4400 vil der blive udført specifikke aftalte arbejdshandlinger og ud fra disse, vil der være resultat ud fra hver af de aftalte handlinger.	Ved udførelse af ISRS 4400 afgiver revisor ikke en konklusion, da det er op til modtageren at konkludere.

Internationale standarder indenfor revision

International Standard on Assurance Engagements (ISAE), International Standards on Auditing(ISA) og International Standard on Related Services (ISRS) er standarder som er udarbejdet og godkendt af International Auditing and Assurance Standards Board (IAASB) samt The International Federation of Accountants (IFAC).

IAASB blev oprettet i 1978, og deres formål er at opretholde en høj standard indenfor standarder vedrørende revision, andre erklæringsopgaver med sikkerhed og beslægtede opgaver.

Ligesom revisors formål er det også IAASBs formål at være med til at sætte offentlighedens interesser i front, samt at være med til at sørge for at nationale standarder ligner internationale standarder. Det er med til at gøre revisionsarbejdet mere ens, når der bliver arbejdet på internationalt plan og dermed øger det tilliden til revisors arbejde på et mere globalt plan[40].

På det nationale plan udarbejdede FSR i 1978 Revisionsteknisk Udvalg (REVU). Det er deres opgave at udarbejde, hvad der i starten blev kaldt Revisionsvejledninger, som senere blev til Revisionsstandarder og i 2009 omdøbt til ISA, ISRE, ISE og

[39] ISRS 4400
[40] ISAE 3000

ISRS. Disse standarder er udarbejdet ud fra de internationale standarder som IAASB udsendte, som omhandler revision, andre erklæringsopgaver med sikkerhed og beslægtede opgaver. De trådte i kraft i Danmark i 2011, da FSR skulle oversætte standarderne til dansk og IFAC fastsatte tidspunktet for ikrafttrædelse. Ydermere skulle standarderne godkendes af EU efter retningslinjer fastsat af IFAC. Direktiv 2006/43/EF, artikel 26. punkt 1 er regelgrundlaget for, hvornår revisor skal følge de internationale standarder:

> *"Medlemsstaterne bestemmer, at revisorer og revisionsfirmaer udfører lovpligtig revision i overensstemmelse med de internationale revisionsstandarder, som Kommissionen har vedtaget efter proceduren i artikel 48, stk. 2. Medlemsstaterne kan anvende en national revisionsstandard, så længe Kommissionen ikke har vedtaget nogen international revisionsstandard, der dækker samme emne. Vedtagne internationale revisionsstandarder offentliggøres i deres helhed på alle Fællesskabets officielle sprog i Den Europæiske Unions Tidende."*[41]

ISAE 3000

"ISAE 3000 Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger"[42], trådte i kraft den 15. december 2015 og gælder erklæringer med sikkerhed fra den 15. december 2015 og senere. ISAE 3000 omhandler andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger, som bliver behandlet ud fra de gældende ISA og ISRE. ISAE 3000 er derfor ikke gældende, når det drejer sig om andre erklæringsopgaver med sikkerhed. ISA og ISRE kan dog være med til at give vejledning ved udførelse af opgaven (jf. ISAE 3000, afsnit A21-A22)[43].

Udførelse af erklæringsopgaver med sikkerhed gælder både attestation opgaver og direkte erklæringsopgaver. Det handler om, at revisor selv måler eller vurderer

[41] EU Direktiv, 2006
[42] ISAE 3000
[43] ISAE 3000

erklæringsemnet efter kriterierne i de direkte erklæringsopgaver, eller om anden anden part gør det i attestations opgaver. Det er gældende regler ved udførelse af begge opgaver jf. ISAE 3000, A30-34 samt A61-A66.

> *"*[...] *opgaveteamets medlemmer og kvalitetssikringskontrollanten (ved opgaver, hvor der er udpeget en sådan) er omfattet af Del A og B i IESBA's Etiske regler vedrørende erklæringsopgaver med sikkerhed eller andre faglige krav eller krav i lov eller øvrig regulering, der er mindst lige så krævende."*[44]

Samt

> *"*[...] *den revisor, der udfører opgaven, er beskæftiget i et firma, der er underlagt ISQC 1 eller andre faglige krav, eller krav i lov eller øvrig regulering vedrørende firmaets ansvar for sit kvalitetsstyringssystem, som er mindst lige så krævende som ISQC 1"*[45]

Når en erklæringsopgave med sikkerhed bliver udført under ISAE'erne kan både være en erklæringsopgave i sig selv, eller være en del af en større opgave, hvor den derfor kun vil være relevant ved de dele af opgaven, som omhandler erklæringen med sikkerhed.

Er erklæringsopgave med sikkerhed ud fra ISAE'erne er en opgave, hvor det er revisors mål at opnå en høj grad af sikkerhed og sikre sig at de informationer, revisor har til rådighed ikke indeholder nogen væsentlig fejlinformation, hvor revisor derefter kan lave en konklusion:

> *"*[...] *en konklusion om udfaldet af målingen eller vurderingen af erklæringsemnet i en skriftlig rapport, hvori der enten formidles en konklusion med høj grad af sikkerhed eller en konklusion med begrænset sikkerhed, og som beskriver grundlaget for konklusionen (jf. afsnit A2), og at kommunikere*

[44] ISAE 3000
[45] ISAE 3000

> *yderligere, som det kræves af denne ISAE og eventuelt andre relevante ISAE'er."*[46]

Revisors opgave er derfor i erklæringer med sikkerhed at opnå en høj grad af sikkerhed for, at han kan give sin konklusion. I scenariet hvor revisor ikke kan opnå den høje grad af sikkerhed, skal revisor ifølge ISAE undlade at give en konklusion, eller helt trække sig for opgaven, hvis loven tillader det.

Ved udførelsen af ISAE 3000 og ved at de områder som erklæringen omhandler, drejer sig om outsourcede persondata, bliver kunden derfor i den situation den dataansvarlige og outsourcing-leverandøren bliver databehandleren. I disse situationer har FSR, Cybersikkerhedsudvalg vurderet, at det vil kræve en erklæringsskabelon, som kan danne udgangspunkt for fremtidige erklæringer om design, implementering og effektivitet af de kontroller[47]. I disse situationer hvor det omhandler persondata og dermed GDPR kræver det, at man er ekstra opmærksom på, hvem der er dataansvarlig, samt hvem der er databehandleren. Skabelonen for erklæringen har til formål at sikre databehandlerens behandling af personoplysninger, som den dataansvarlige er ansvarlig overfor. Erklæringsskabelonen vil blive tilpasset, når lovkravene med de nationale bestemmelser vedtages.

ISAE 3402

ISAE 3402, "Erklæringsopgaver med sikkerhed om kontroller hos en serviceleverandør"[48] trådte i kraft den 15. juni 2011 og gælder alle serviceleverandørers revisorers erklæringer med sikkerhed fra den 15. juni 2011 og senere.

ISAE 3402 handler om revisors arbejde ved udførelsen af en erklæring, der benyttes af brugervirksomheder og disses revisorer vedrørende kontrollerne hos en

[46] ISAE 3000
[47] Mogensen, 2018
[48] ISAE 3402

serviceleverandør[49]. De leverandører leverer en ydelse til brugervirksomheden, som revisoren skal kontrollere, da det kan have en indflydelse på brugervirksomhedens interne kontroller.

ISAE 3402 er ligesom ISAE 3000, når det kommer til udførelse af erklæringsopgaver med sikkerhed, skal det altid være med en høj grad af sikkerhed, samt at Del A og B i IESBA's Etiske Regler vedrørende erklæringsopgaver med sikkerhed stadig gælder. Til forskel for ISAE 3000 gælder den kun attestation opgaver, da hele ISAE handler om service leverandører. Den kan stadig være supplerende til en større opgave eller ved udarbejdelsen af ISA 402. Det er dog ikke alle erklæringsopgaver med sikkerhed den gælder for, den gælder ikke for:

"[...] *hvor der kun skal afgives erklæring om hvorvidt en serviceleverandørs kontroller har fungeret som beskrevet."*[50]

Eller

"[...] *hvor der skal afgives erklæring om andre kontroller hos en serviceleverandør end dem, der vedrører en ydelse, som sandsynligvis er relevant for en brugervirksomheds interne kontrol, der vedrører regnskabsaflæggelsen (f.eks. kontroller, der påvirker en brugervirksomheds produktion eller kvalitetskontrol)."*[51]

Disse erklæringer med sikkerhed ligger under ISAE 3000, men selve ISAE kan dog være med til at hjælpe ved udførelsen af ISAE 3000. I tilfælde af at udførelsen af ISAE 3402 sker i forbindelse med ISAE 3000, gælder de samme regler for service leverandørens revisor ved udførelsen af arbejdet hos en serviceorganisation, samt at ISAE 3402 kun er med til at supplere ISAE 3000.

Når revisor udfører en revisionserklæring i form af ISAE 3402, er målet for erklæringen at lave et grundlag for de kriterier, der er for at opnå en høj grad af sikkerhed for de punkter, som erklæringen skal give et billede af. Det handler om at

[49] ISAE 3402
[50] ISAE 3402
[51] ISAE 3402

give et retvisende billede af, om der er ordentlige IT-forhold hos en serviceleverandør en den anførte periode, i form af lovkrav samt god IT-skik. For nogle virksomheder kan det være at de af lov skal have udført en ISEA 3402, for andre kan det være de gerne vil give et billede af, at deres virksomhed er en sikker løsning for kunder eller potentielle kunder.

Det gælder derfor om, at revisors erklæring giver et billede af virksomheden, men en høj grad af sikkerhed. Dette kan opnås ved at gennemgå de kontroller, virksomheden har anført og dermed give et billede af, hvordan de generelle tilstande er i IT-systemet, som enten er en del af eller kan påvirke den finansielle rapportering. Dette kan være drift, beredskab, dokumentation, udvikling eller lignende. Kontrollerne, der er omfattet af erklæring, skal derfor også fungere effektivt i forhold til at give et retvisende billede af de kontrolmål, der er i beskrivelsen af service leverandørens beskrivelse af systemet.

En god måde at få overblik over hvilke dele af IT-systemet, der bliver leveret af en outsourcing leverandør til revisors kunde, er at lave en gennemgang af den kontrakt, der er imellem outsourcing leverandør og kunden. Det kontraktuelle grundlag vil som regel bestå af en hovedaftale med bilag og løbende tilføjelser samt en såkaldt service level agreement (SLA), og dermed et overblik over hvilke dele af IT-systemet der er under erklæringen.

Erklæringens begrænsninger er, at det kun kigger på det relevante i forhold til regnskabsaflæggelsen og ikke den samlede IT-sikkerhed eller alle risici i tilknytning til outsourcingen. ISAE 3402 er lavet til at være fleksibel, og derfor er der ikke et generisk sæt af kontrolmål til brug for ISAE 3402 erklæringer, og der anvendes mange variationer heraf. Disse skal altid tilpasses og vurderes i den konkrete situation. Det vil under alle omstændigheder være relevant at foretage en afstemning mellem virksomhedens egne kontrolmål og de, der er anvendt i erklæringerne, både for at afgøre væsentlighed og for at sikre, at fuldstændigheden er på plads.

ISRS 4400

ISRS 4400 "Aftalte arbejdshandlinger vedrørende regnskabsmæssige oplysninger og yderligere krav ifølge dansk revisorlovgivning" er udviklet af IFAC og oversat til dansk af FSR, som har tilføjet yderligere krav ifølge dansk revisorlovgivning. ISRS 4400 trådte i kraft med virkning for erklæringer, der afgives 1. juli 2012 og senere.

Formålet med ISRS 4400 er at give revisor en vejledning samt opstille nogle standarder, som revisor skal bruge i aftalte arbejdshandlinger vedrørende regnskabsmæssige oplysninger og om form og indhold af den erklæring. Revisor kan så derfor ud fra de aftalte arbejdshandlinger udføre arbejdshandlinger vedrørende udvalgte dele af regnskabsmæssige oplysninger, en regnskabs komponent, opgaver om ikke-regnskabsmæssige oplysninger og helt op til et fuldstændigt regnskab.

"[...] *at revisor udfører revision lignende arbejdshandlinger, som revisor, virksomheden og enhver relevant tredjepart er blevet enige om, og erklærer sig om de faktiske resultater."*[52]

ISRS findes i mange forskellige versioner og kan på mange måde bruges på samme måde som ved udførelse af erklæringer efter ISAE 3402 og 3000.

Til forskel for ISAE 3402 og 3000, kræver det ved brug af aftalte arbejdshandlinger vedrørende regnskabsmæssige oplysninger, at revisor har et højt vidensniveau om ydelser og kontrolaktiviteter hos kunden.

"Den kan imidlertid være retningsgivende ved opgaver om ikke-regnskabsmæssige oplysninger under forudsætning af, at revisor har tilstrækkeligt kendskab til det pågældende område." [53]

[52] ISRS 4400
[53] ISRS 4400

Det, som ISRS 4400 derimod kan gøre, er at give en forhøjet effektivitet i forhold til at dække kunden og kundens revisors informationsbehov, da informationsniveauet på forhånd skal være højt.

"Da ovennævnte arbejdshandlinger hverken er revision eller review i overensstemmelse med internationale standarder om revision eller om review og yderligere krav ifølge dansk revisorlovgivning udtrykker vi ikke nogen grad af sikkerhed om kreditorerne pr. (dato)."[54]

Ved brug af ISRS 4400 skal man være opmærksom på at ved udførelsen af arbejdshandlingerne er det op til modtageren at lave en konklusion af arbejdshandlinger, og revisor kommer derfor ikke med sin egen konklusion. Derfor er ISRS 4400 ikke en erklæring med sikkerhed.

Cyberkriminalitet

Cyberkriminalitet er en overordnet beskrivelse af kriminelle aktivitet, som sker i den digitale verden. Det dækker over en lang række forskellige måder, hvorpå ondsindede aktører enten prøver at tilskaffe sig adgang til IT-systemer eller data. IT-kriminelle kan også have en aktivistisk tilgang, hvor det ikke drejer sig om at "stjæle" men at såre virksomheden for at fremme en sag.

Det Kriminalpræventive Råd opdeler cyberkriminalitet (også kaldt IT-kriminalitet) i tre kategorier, som hver indeholder forskellige former for angreb: Computerintegritetsforbrydelser, Computerassisterede forbrydelser samt Computerindholdsforbrydelser[55].

Computerintegritetsforbrydelse er forbrydelser hvor ondsindede aktører angriber IT-systemerne direkte. Disse angreb er tit rettet mod virksomheder for at få adgang til deres systemer: Af typer af angreb ses hacking, ddos-attacks, malware, ransomware og trojanske heste.

[54] ISRS 4400
[55] Det Kriminalpræventive Råd, 2020

Malware er en oversigt over malicious software, som kan inficere en computer og dermed enten skade IT-systemerne eller gøre at computeren ikke længere virker, som den skal.

Malware kan være en del af brugen af ransomware, hvor ondsindede aktører skaffer sig adgang til computeren ved brug af malware og derefter låser den eller gør den utilgængelig, medmindre brugeren betaler de ondsindede aktører.

Computerassisterede forbrydelser er forbrydelser, hvor de ondsindede aktører bruger computeren som et redskab, som en del af deres angreb til at få adgang til systemerne. Af typer af angreb ses identitetstyveri, misbrug af betalingskort, nethandelsbedrageri, phishing samt social engineering.

Phishing er en af de mest hyppige former for angreb, som sker. Her "fisker" de ondsindede aktører efter informationer. Dette kan ske enten ved brug af mails, sms eller telefonopkald.

De ondsindede aktører kan f.eks. sende en sms, som ligner at den kommer fra Nets eller ens bank og dermed virke som en legitim besked i håbet om at skaffe enten adgang eller informationer ud af brugeren. Dette kan være nemid, cpr-nummer, kreditkortsinformation eller lignende.

Social engineering er hvor de ondsindede aktører enten ved brug af identitetstyveri eller ved at skabe en slags tillid hos brugeren, gør sådan at brugeren enten selv udfører viljen af de ondsindede aktører eller frivilligt overgiver informationer.

Finansiel svindel kan ske ved at medarbejderne selv, ved brug af computeren eller software, enten prøver at manipulere tallene eller en anden form for svindel for deres egen vindings skyld. Dette kan ske i form af regnskabsmanipulation eller lign.

I flere af disse tilfælde er der høj chance for at fortrolige og følsomme personoplysninger eller anden fortrolig information utilsigtet blevet delt, hvilket kan skade virksomhedens brand samt kan betyde store økonomiske tab.

Computerindholdsforbrydelser omhandler opbevaring af ulovligt materiale, hvilket ikke er relevant for dette speciale.

Hvor er sårbarhederne?

Cybersikkerhedsrådet kom med den seneste nationale strategi for cyber- og informationssikkerhed i 2018 og gælder til 2021[56]. Her skriver de bl.a.:

> *"Truslerne på cyber- og informationssikkerhedsområdet påvirker alle dele af samfundet."*[57]

I den nationale strategi beskriver rådet de fem sårbarheder, som danske borgere og virksomheder skal være opmærksomme på, når de færdes i den digitale verden:

1. Utilstrækkelig sikkerhedsadfærd,
2. Stor afhængighed af digital infrastruktur,
3. Flere enheder er forbundet,
4. Stor kompleksitet i IT-porteføljen samt
5. At cyberangreb kan udføres let og billigt.[58]

De fem sårbarheder gennemgås punkt for punkt i nedenstående.

Utilstrækkelig sikkerhedsadfærd

Utilstrækkelig sikkerhedsadfærd gælder for både borgere og virksomheder, som enten ikke er opmærksomme på de angreb, som ondsindede aktører udfører, eller som ikke har fået den tilstrækkelige træning til at kunne håndtere et eventuelt angreb.

> *"I myndigheder og virksomheder er ledere og medarbejderes sikkerhedsmæssige adfærd afgørende for at opnå et passende beskyttelsesniveau.*[59]*"*

[56] Regeringen, 2018
[57] Regeringen, 2018
[58] Regeringen, 2018
[59] Regeringen, 2018

Stor afhængighed af digital infrastruktur

Når virksomheder og borgere bliver mere og mere afhængige af den digitale verden, kan det ske, at brugeren muligvis kan går lidt for hurtigt frem og med en mulig dumdristig tilgang til udvidelsen af systemer. Det kan føre til svagheder i systemet, kombineret med en store pålidelighed overfor den digitale verden og derfor er det kritisk, at man får etableret den korrekte infrastruktur for at borgere og virksomheder kan færdes forsvarligt i den digitale verden uden at påføre andre eller sig selv skade.

"Manglende tilgængelighed, integritet og fortrolighed i den digitale infrastruktur kan medføre betydelige konsekvenser for samfundet."

Flere enheder er forbundet

I takt med at brugerne får en større afhængighed af den digitale verden, stiger antallet af enheder også. Antallet af enheder og muligheder som brugerne bliver udsat for stiger i takt med at f.eks. kan medarbejderen have et smart home med wifi tilkoblede lamper, digital assistent i form af Google home eller Apples siri. Ved at man får flere og flere enheder stiger antallet af adgangspunkter for de ondsindet aktører:

> *"Når systemer og infrastruktur bliver stadig mere integrerede, bliver sikkerhedsudfordringerne mere komplekse"*[60].

Stor kompleksitet i IT-porteføljen

Når offentlige organisationer og private virksomheder bevæger sig frem i den digitale verden, er det vigtigt fortsat at have overblik over, hvad ens IT-portefølje faktisk indeholder. Det kan være, at virksomheden har et gammelt system, som ikke er brug længere, men som stadig har adgang til kritiske informationer i virksomheden. Denne høje kompleksitet kan skabe sårbarheder ved at have for komplekse og uoverskuelige IT-systemer, og derfor har virksomheden ikke cybersikkerheden til at beskytte alle punkter.

[60] Regeringen, 2018

Cyberangreb kan udføres let og billigt

De ondsindede aktørers mulighed for nemt og billigt at anskaffe sig hardware og software, som gør det muligt at udføre et angreb, er steget relativt meget. Om det er callcentre, hvis eneste formål er at lade som om de er Windows support center eller social engineering, kan disse angreb udføres fra simple computere og telefoner. Større angreb i form af DDoS kan ske ved brug af adgang til flere tusinde computere og dermed skabe store problemer for virksomheder, kun ved brug af nemt tilgængeligt hardware.

Cybersikkerhed [61][62][63]

Cybersikkerhed er de foranstaltninger, som bliver gjort for at sikre virksomheder, offentlige organisationer samt borgere imod de angreb, som ondsindede aktører prøver at udføre mod dem. Cybersikkerhed handler både om at sikre IT-systemer imod angreb i form af VPN, firewall eller andet antivirus software, men også om at gøre brugeren opmærksom på de trusler, der findes.

VPN (virtuel private network) gør, at ens IP-adresse ikke kan spores til et specifikt punkt. Det kan give adgang til en mere sikker brug af hjemmesider og det kan sikre brugerens identitet.

Firewall er med til at give computere en sikring mod udefrakommende angreb. Den sorterer i din internetforbindelse, hvilke adgang der er lovlige og hvilke den skal blokere for.

Antivirus eller malware detection giver computeren et forsvar i tilfælde af, at computeren bliver angrebet. Det kan være med til at opspore eller identificere inficerede programmer eller filer.

[61] Cybercrime Survey 2019, 2019
[62] Regeringen, 2018
[63] Det Kriminalpræventive Råd, 2020

Som tidligere nævnt er brugeren den største trussel, og det er derfor ekstremt vigtigt at informere brugeren og give dem den nødvendige træning, der kræves for at færdes sikkert i den digitale verden. En måde at sikre systemerne overfor brugeren på kan være gennem awareness træning, to-faktor verifikation, privilegeret adgangsstyring samt identitets- og adgangsstyring. Disse systemer vil blive gennemgået i nedenstående.

Awareness træning er undervisning af brugeren ift. hvilke trusler der findes og hvordan de skal agere i den digitale verden. Dette kan ske i form af envejskommunikation ved f.eks. brug af plakater eller lignende eller ved at have fysisk undervisning eller e-learning.

To-faktor verifikation kender de fleste fra NemId. Det giver brugeren, udover at have sit kodeord, en form for fysisk sikring. Dette kan også være i form af en sms men en unik kode for hver gang man skal logge ind.

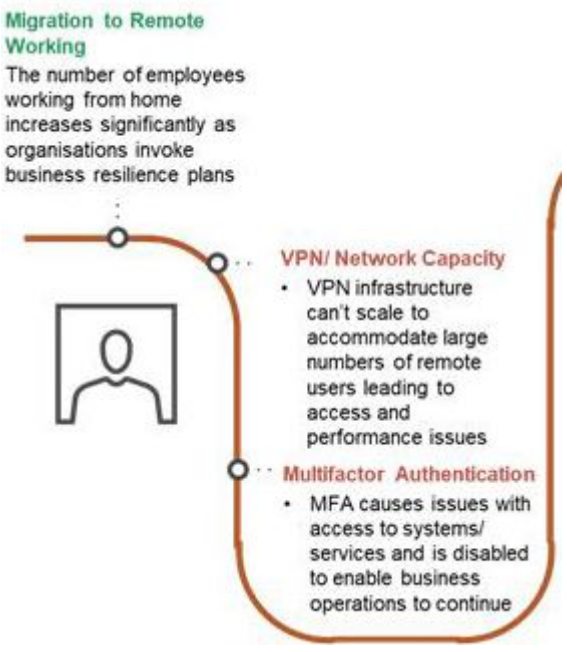
Privilegeret adgangsstyring giver bruger adgang til de informationer, data samt programmer, som brugeren skal have adgang til, men ikke flere end nødvendigt. Det er f.eks. vigtigt, at hvis en ansat har været i flere afdelinger, at de så ikke har adgang til dem alle sammen, men kun der, hvor der er et behov. Derfor er privilegeret adgangsstyring en slags begrænsning af brugerens adgang og dermed handlemuligheder og adfærd i systemerne. Dette er med til at begrænse omfanget af de skader, der kan ske, hvis endeligt et angreb sker.

Identitets- og adgangsstyring er en måde at sikre, at en bruger nu også er den korrekte og at brugeren har adgang til de informationer, som brugeren har rettighed til. Det kan ske i form af at automatisere virksomhedens identiteter og dermed sikre at der ikke kan ske en menneskelig fejl, da det ikke er en manuel kontrol.

Webinar: Cyber Security-udfordringer i krisetider[64]

PwC har i forbindelse med udførelsen af deres CFO Pulse Survey[65] også lavet et webinar, som skal give et indblik i resultaterne af undersøgelsen og de udfordringerne, der er under krisetider. Den tager derfor udgangspunkt i den data, der er i CFO Pulse Survey. Derudover ser de på, hvilke problemer deres kunder oplever på globalt plan. Den giver derfor indsigt i, hvordan situationen er ude i virksomhederne samt hvordan krisen påvirker cybersikkerheden. Værterne for webinaret er Mads Nørgaard Madsen, partner i PwC samt Head of Security and Technology og Natasha Lembke, partner i PwC og Head of Finance Transformation.

Formålet med dette webinar er at er få et indblik i økonomidirektørens bekymringer, hvilke tiltag det giver mening at gøre under corona-krisen og hvilke udfordringer PwC ser.



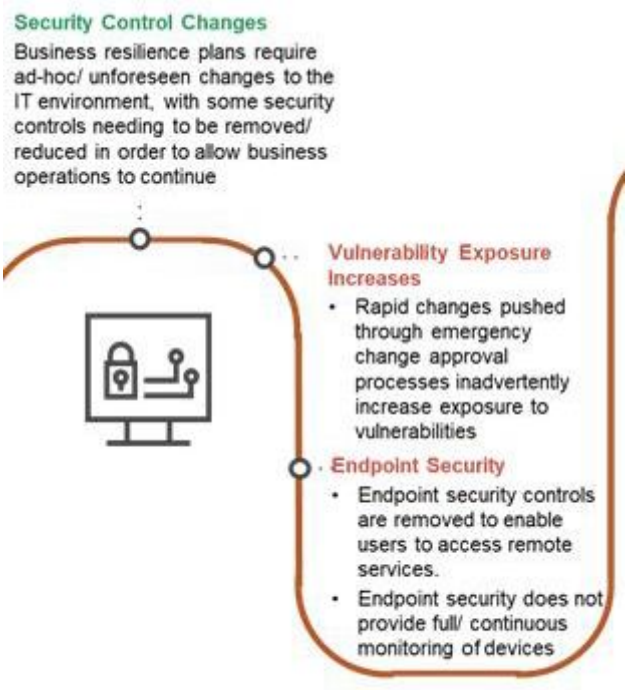
Det første udfordring, som PwC ser, er at mange medarbejdere vil tage deres arbejdsplads med hjem, så de så vidt muligt stadig kan udføre deres arbejde. [66] Udfordringen med dette er, at virksomhedens IT-systemer vil blive sat under et stort pres, som systemerne måske ikke har den rette infrastruktur til. Her bliver der nævnt VPN og netværksadgang. Disse funktioner skal give medarbejderen adgang til virksomhedens netværk enten i form af et fjernskrivebord eller en server adgang. Virksomheder som ikke har sat de rette

[64] PwC, Cybersecurity-udfordringer i krisetider, 2020
[65] PwC, COVID-19 CFO Pulse Survey, 2020
[66] PwC, Cybersecurity-udfordringer i krisetider, 2020

procedurer i værk, inden corona-krisen vil opleve en udfordring i form af en øget trafik.

Ydermere ser de to-faktor verifikation som en udfordring ift. hjemmearbejde. Virksomheder, som ikke har sat en to-faktor verifikation op inden krisen, kan stå i situationer, hvor medarbejdere ikke kan få adgang til de rette systemer og data, og derfor ikke kan udføre deres arbejde.

[67]

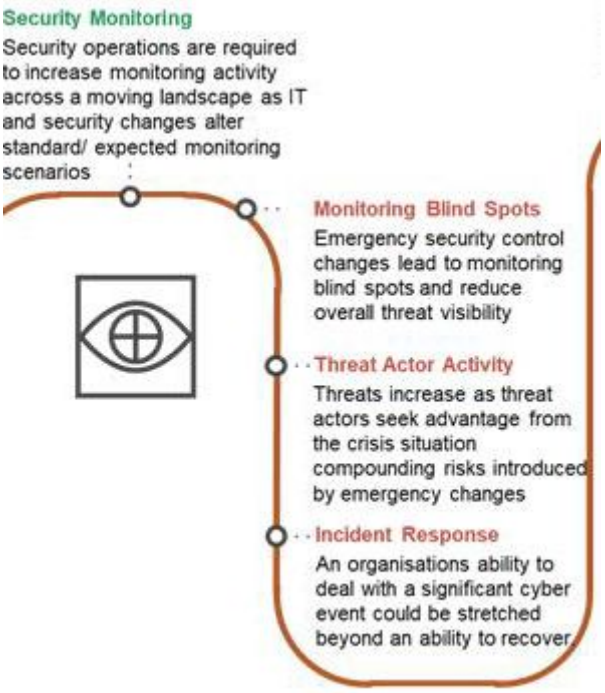


Anden del af de udfordringer, som PwC udpeger i webinaret er sikkerhedskontrol ændringer. IT-systemer præ corona-krisen er simpelthen ikke sat op til at kunne fungere med den store belastning på systemerne. Der vil derfor under krisen blive lavet ændring i IT-sikkerhedskontroller løbende for at sørge for, at medarbejdere får adgang til de rette programmer eller data. Det kan endda være, at der vil blive ophævet eller væsentlig reduceret i disse kontroller.

Disse ændringer kan være med til at skabe flere sårbarheder i virksomhedens IT-systemer. Dette kan ske som følge af, at virksomheden for hurtigt og uden at gennemtænke de mulige konsekvenser af deres ændringer.

Dette kan være i form af Endpoint sikkerhed, hvor medarbejderne får fjernadgang og virksomheden ikke har en overvågning af medarbejderens handlinger. Endpoint sikkerheden bliver derfor udsat for et kompromis i forhold til at vedligeholde sikkerheden eller arbejdsgangene.

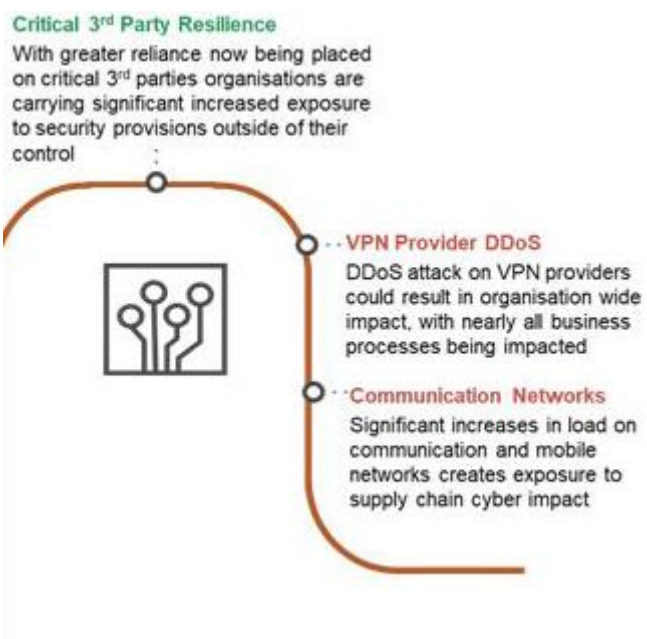
[67] PwC, Cybersecurity-udfordringer i krisetider, 2020



Tredje punkt, som PwC udpeger som udfordringer, som corona-krisen bringer med sig, er overvågning af trusler og sikkerhed. Ved at sikkerheden i følge af endpoint, en stigning i aktivitet og at sårbarheden stiger, kræver det, at virksomhederne øger deres overvågningskapaciteter. Virksomheden skal derfor til at "løbe" hurtigt for at finde de trusler, der nu kan være, og derfor kan det være med til at skabe huller i deres overvågning. Blinde vinkler i virksomhedens overvågning skaber muligheder, som ondsindede aktører kan udnytte.[68]

Ondsindede aktører ser derfor denne krisetid som en mulighed for at finde og udnytte disse blinde vinkler, og formodentligt derfor ses en stigning i disse aktøreres aktiviteter. Virksomhederne kan derfor se en række udfald af disse mulige angreb. De skade, som de IT-kriminelle kan forvolde, kan være store og i værste tilfælde helt lægge virksomheden ned. PwC argumenterer for, at det derfor er kritisk, at virksomhederne øger overvågning og på bedst mulig vis sikrer, at der ikke er nogle blinde vinkler i deres systemer.

[68] PwC, Cybersecurity-udfordringer i krisetider, 2020



Den fjerde udfordring som PwC udpeger i webinaret er tredjeparts sikkerhed. Når hele virksomheden indenfor kort tid skal have adgang til en VPN kan det sætte store krav til VPN-udbyderen. Disse tredjeparts virksomheder bliver udsat for et pres under corona-krisen og ved den øgede pres vil der også være ondsindede aktører, som ser muligheder. [69]

Hvis en VPN-udbyder bliver udsat for et DDos angreb og hele deres service bliver lagt ned, kan det skabe større udfordringer for alle de virksomheder, som anvender deres service.

Den digitale infrastruktur vil også blive sat på prøve, da antallet af brugere og dermed aktivitet vil stige. Derfor ser man f.eks. også, at Netflix i samarbejde med EU har sat kvaliteten ned på dele af deres streaming service for at sænke presset på internet infrastrukturen[70].

Ransomware

På webinaret omtalte PwC også ransomware. I 2020 har ondsindede aktører været meget aktive og især ved brug af ransomware. Under corona-krisen har der været flere phishing- og ransomware-kampagner, som alle har temaet coronavirus. Det er en mulighed for at lave en relevant og iøjnefaldende kampagne, som i en krisetid kan lokke flere i fælden. Allerede fra januar blev der set eksempler på mails og lignende som havde coronavirus som tema.

[69] PwC, Cybersecurity-udfordringer i krisetider, 2020
[70] Politico EU, 2020

Rasmus Madsen Carlslund
Cand.merc.aud.
Den 31. maj 2020

71

Den ovenstående hjemmeside er et eksempel hvor legitime hjemmesider bliver brugt som et skjul for malware. De bruger den tillid, brugerne allerede har til forskellige hjemmesider til at lokke folk til at "åbne" mere op og dermed tillade mere.

[71] PwC, Cybersecurity-udfordringer i krisetider, 2020

Rasmus Madsen Carlslund
Cand.merc.aud.
Den 31. maj 2020

Analyse

Formålet med specialets analyse er at analysere, hvordan det danske erhvervsliv generelt og specifikt forholder sig til cyberkriminalitet og cybersikkerhed. Derfor vil analysen besvare de to underspørgsmål:

- ➔ **Underspørgsmål 1:** Hvordan håndteres truslen om cyberkriminalitet blandt de danske virksomheder generelt?
- ➔ **Underspørgsmål 2:** Hvordan påvirker corona-krisen cyberkriminalitet og virksomhedernes IT-sikkerhed, og hvordan kan virksomhederne håndtere krisen?

Ift. underspørgsmål 2 besvares den sidste del af spørgsmål først i diskussionen.

Analysen vil tage udgangspunkt i følgende undersøgelser og webinar:

1. Cybercrime Survey 2019 udgivet af PwC
2. CFO Pulse Survey, 2019: Corona-krisens indflydelse på IT-sikkerhed, udarbejdet af PwC
3. Webinar: Cyber Security-udfordringer i krisetider, 2019, lavet af PwC
4. Gartner CIO Survey, 2009, som handler om cybersikkerhed efter Finanskrisen, udarbejdet af Gartner

Helt overordnet set er analysens formål at bidrage til at besvare den overordnede problemformulering, som lyder:

> "*Hvordan sikrer revisorer sig, at virksomhederne lever op til de krav, der er til cybersikkerhed, så de sikkert kan agere i den konstant udviklende digitale verden?*"

Cybercrime Survey 2019

Denne såkaldte Cybercrime Survey[72] er udarbejdet af PWC og har kørt siden 2015. I de fem år har den fulgt hvilke tendenser, der er inden for cyberkriminalitet. Ligeledes har undersøgelsen været med til at give et billede af respondenternes syn på tilliden til cybersikkerhed samt hvordan cyberkriminalitet er med til at påvirke de adspurgtes virksomheder. I de seneste år har den været med til at følge udviklingen af GDPR og hvordan indstillingen til IT generelt har været i årene efter.

I alt er der 325 danske og 71 norske virksomhedsledere, IT-chefer og specialister fra danske virksomheder, der har deltaget i PwC's Cybercrime Survey 2019. Fordelingen af respondenterne er 62 % fra den private sektor, 25 % fra den offentlige og 13 % fra den finansielle sektor.

Undersøgelsen er udviklet med opbakning fra Center for Cybersikkerhed, DI Digital, Finans Danmark, Dansk Erhverv, IT-Branchen, Dansk It, KITA, Rigspolitiet NC3, Microsoft, Rådet for Digital Sikkerhed og ISACA.

Cyberkriminalitetsundersøgelsen bidrager til at skabe en bred forståelse for de forskellige sektorer, som kan blive påvirket af et angreb eller en lignende cyberkriminalitet relateret hændelse. Den brede gruppe af både respondenter samt opbakningen fra store spillere inden for cyberkriminalitet samt IT, er med til at give surveyen en stor troværdighed. Ligeledes kan både den store respondentgruppe og opbakningen fra store spillere i markedet være med til at skabe en tillid til undersøgelsens resultater. Dog skal det nævnes, at PwC leverer løsninger til mange af de problemer, der bliver opstillet i Cybercrime Survey 2019, og derfor skal informationen analyseres med et vis kritisk synspunkt.

Cybercrime Survey 2019 er struktureret ud fra PwC's PAVA-koncept, som dækker over fem hovedområder:

[72] PwC Cybercrime Survey 2019, 2019

1. Governance, risk og compliance
2. Proces
3. Adfærd
4. Validering
5. Arkitektur

Disse fem hovedområder gennemgås i nedenstående.

Governance, risk og compliance-området

Governance, risk og compliance-området er de love, regler og krav, som virksomheden skal have i stand, før de er i compliance. Kravet til compliance gælder også de forskellige sikkerhedsmæssige krav, der kan være for virksomhedens IT-ledelse samt risikostyring. Governance, risk og compliance-området ligger som en ydre ring omkring hele PAVA-konceptet. Det er med til at sætte en standard for hele opbygningen af virksomhedens IT-ledelse samt deres compliance. Det er derfor utrolig vigtigt for virksomheden at være opmærksom på alle de forskellige regler, love og krav, der er, og at virksomheden konstant holder sig opdateret. Governance, risk og compliance-området kan f.eks. være, hvis en virksomhed har en certificering, som de ønsker at opretholde eller der sker ændringer i krav eller retningslinjer fra staten.

Procesområdet

Procesområdet dækker de processer og forretningsgange samt den dokumentation, som virksomheden har etableret, herunder hvordan processer er designet og kommunikeret og om de er effektivt implementeret i virksomheden.

Adfærdsområdet

Adfærdsområdet omfatter niveauet af medarbejdernes bevidstheds- og kompetenceniveau i forhold til virksomhedens sikkerheds- og compliance-krav.

Valideringsområdet

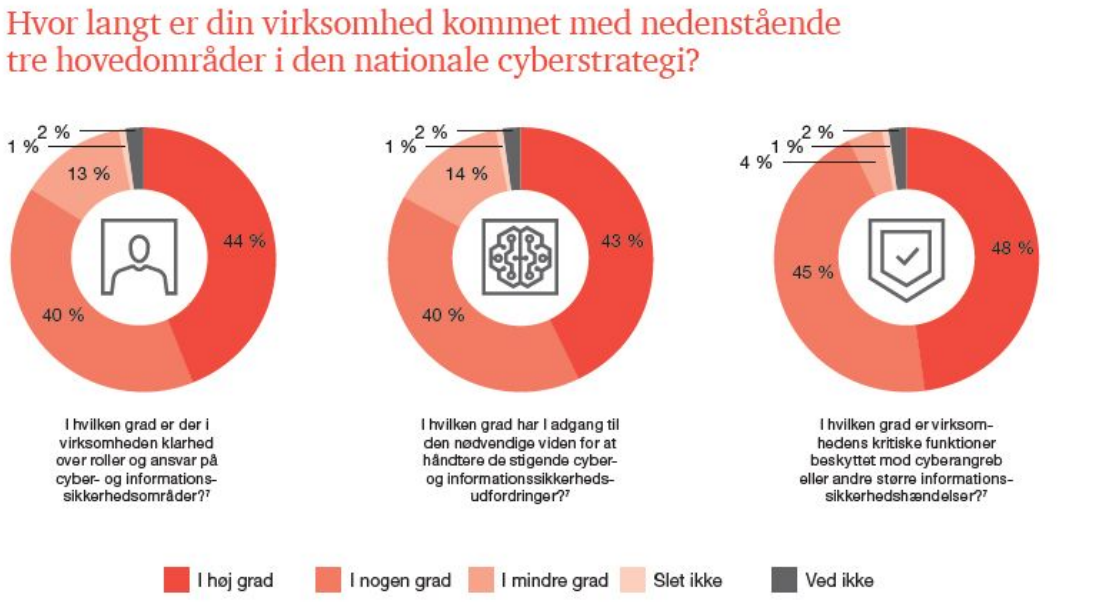
Valideringsområdet beskriver aktiviteter til at opdage og verificere svagheder og sårbarheder i forhold til virksomhedens sikkerheds- og compliance-niveau.

Arkitekturområdet

Arkitekturområdet dækker design, konfiguration og implementering af tekniske og fysiske løsninger i forhold til virksomhedens sikkerheds og compliance-niveau.

Danmarks nationale strategi for cyber- og informationssikkerhed[73]

I 2019 lancerede staten den nationale strategi for cyber- og informationssikkerhed, som består af 25 initiativer samt seks målrettede strategier. Den har til formål at bidrage til at sikre, at de samfundskritiske sektorer såsom tele-, finans-, sundheds-, transport- og søfartssektoren har nogle retningslinjer, som skal være med til at sikre dem mod angreb fra IT-kriminelle. Ud fra alle respondenterne i PwC's Cybercrime Survey 2019 er 47 % af de adspurgte hører ind under de samfundskritiske sektorer såsom tele-, finans-, sundheds-, transport- og søfartssektoren, der, som nævnt, er underlagt Danmarks nationale strategi for cyber- og informationssikkerhed.



74

[73] PwC Cybercrime Survey 2019, 2019
[74] PwC Cybercrime Survey 2019, 2019

I den nationale strategi for cyber- og informationssikkerhed bliver der sat tre pejlemærker, som i de næste par år skal hjælpe de danske virksomheder med at komme bedre og mere sikkert frem i den digitale verden. Det drejer sig om en fælles indsats, bedre kompetencer samt en tryg hverdag for borgere og virksomheder. I cyberkriminalitetsundersøgelsen blev der spurgt:

> *"I hvilken grad er der i virksomheden klarhed over roller og ansvar på cyber- og informationssikkerhedsområder?"*

44 % af de adspurgte har i høj grad en klarhed over rollerne og ansvaret inden for cyber- og informationssikkerhed, mens 40 % i nogen grad har. Dog har 13 % af de adspurgte i mindre grad klarhed over det. Der er tale om 1 %, som slet ikke har klarhed over rollerne og ansvaret.

Tallene antyder, at de adspurgte i nogen eller høj grad har en klarhed over deres roller og ansvar. Denne klarhed og ansvarsfordeling kan være med til at skabe nogle klare linje for den indsats, der skal til for at kunne forberede sig på et cyberangreb. Ansvarsfordelingen kan være kritisk, når medarbejdere skal identificere trusler og skabe fælles front mod ondsindede aktører.
I undersøgelsen blev følgende spørgsmål også stillet:

> *"I hvilken grad har I adgang til den nødvendige viden for at håndtere de stigende cyber og informationssikkerhedsudfordringer?"*

43 % af de adspurgte har i høj grad adgang til den nødvendige viden til at håndtere udfordringer inden for cyber- og informationssikkerhedsområdet. 40 % har i nogen grad adgang mens 14 % i mindre grad har adgang til den nødvendige viden. Der er tale om 1 %, som slet ikke har den nødvendige viden.

Tallene i undersøgelsen antyder jf. de adspurgte i nogen grad eller høj grad har adgang til den viden, der skal bruges til at håndtere en mulig cyberudfordring. Med adgang til den nødvendige viden kan medarbejdere hurtigt og sikkert være med til at identificere de trusler, der muligt kan komme, men også reagere hurtigere hvis uheldet er ude. Behovet for at have medarbejdere med de korrekte kompetencer, samt en konstant opdatering af de kompetencer, er vigtig for at kunne håndtere den digitale verden. Derfor vil specialet argumentere for, at det at have medarbejdere med adgang til den nødvendige viden er essentielt for det danske erhvervsliv.

Et tredje spørgsmål, der blev stillet i den nationale undersøgelse:

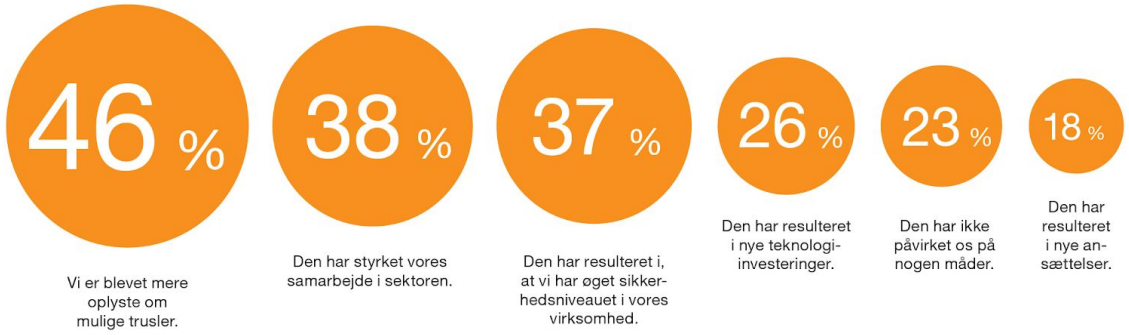
> *"I hvilken grad er virksomhedens kritiske funktioner beskyttet mod cyberangreb eller andre større informationssikkerhedshændelser?"*

48 % af de adspurgte mener, at virksomhedens kritiske funktioner er beskyttet mod cyberangreb eller andre større informationssikkerhedshændelser. 45 % mener i nogen grad at de kritiske funktioner er beskyttet mod angreb, mens 4% i mindre grad mener det. Der er tale om 1%, som slet mener, at virksomheden er beskyttet mod et cyberangreb.

Tallene antyder jf. de adspurgte, at der i nogen eller høj grad er beskyttet mod cyberangreb eller andre større informationssikkerhedshændelser. At vide, hvad virksomheden skal beskytte og have en strategi for, hvordan virksomheden beskytter det korrekt, er essentielt for at kunne modstå et cyberangreb. Det høje antal, der mener de er beskyttet, er med til at sikre, at staten og samfundskritiske sektorer forbereder sig på det skiftende trusselsbillede og at de er i stand til at beskytte væsentlige samfundsmæssige funktioner mod cyberangreb eller andre større informationssikkerhedshændelser.

Dog er det vigtig at vide, at den digitale verden er konstant skiftende og virksomhederne skal derfor hele tiden være på vagt. Derfor betyder den høje grad af

sikkerhed inden for området ikke, at man kan begynde at slappe af eller sænke forsvaret. Cybersikkerhed er en skiftende størrelse og angreb tager hele tiden nye former.



75

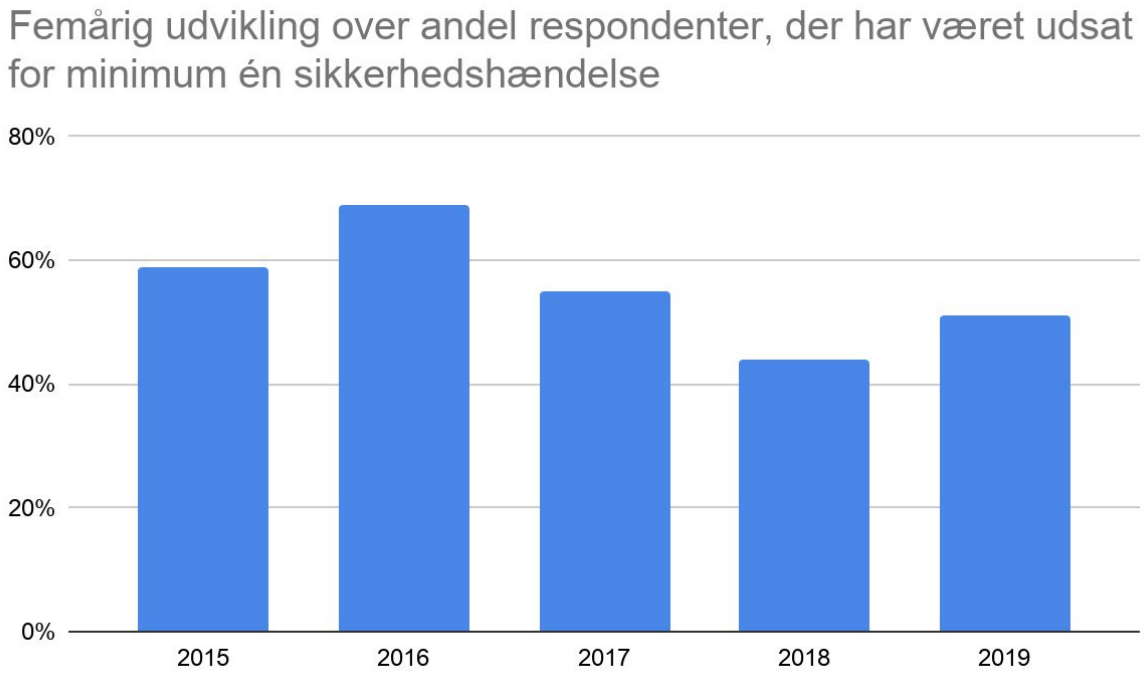
Hvis man ser på antallet af de adspurgte, mener 46 %, at de er blevet mere oplyste i forhold til de mulige trusler, der er. 37 % af de adspurgte har øget deres sikkerhedsniveau. Det kan derfor betyde, at den nationale strategi er med til at skabe bedre rustede virksomheder overfor eventuelle kommende cyberangreb.

At have en national strategi for cyber- og informationssikkerhed er ikke en helhedsgardering mod cyberangreb, men med en fælles strategi og plan mod cyberangreb vil staten prøve at sikre det danske samfund og erhvervsliv samt de samfundskritiske sektorer inden for cyber- og informationssikkerhed. Det skal være med til at sikre, at det danske samfund fortsat kan være med i den digital verden, som er i konstant forandring.

Antal udsat for angreb

Andelen af respondenter, der i løbet af de seneste fem år har været udsat for minimum et angreb, er ifølge undersøgelsen 51 % i 2019. Dette er en stigning på 7 % i forhold til 2018, hvor tallet var 41 %.

[75] PwC Cybercrime Survey 2019, 2019

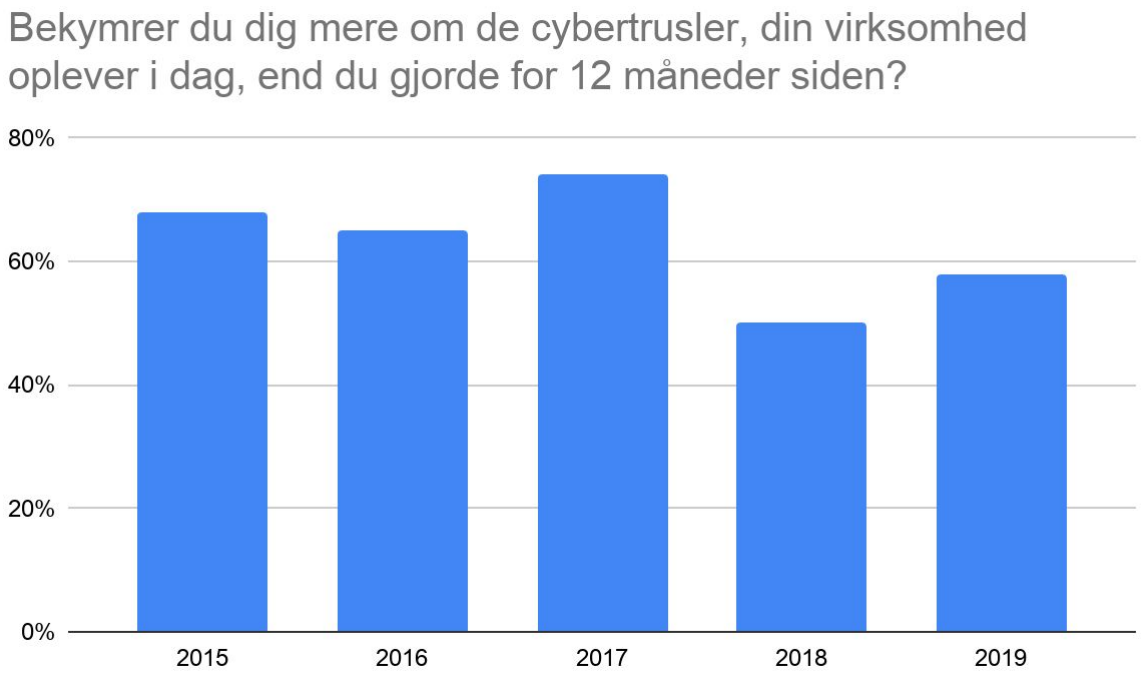


[76]

År 2019 er med til at ændre kurven, da der siden 2016 har været en faldende tendens, hvor færre virksomheder var udsat for angreb. Det kan muligvis skyldes indførelsen af GDPR i maj 2018, som kan have til store økonomiske sanktioner som følge, hvilket formentligt har været med til at skabe en forhøjet indsats på IT-området og dermed cybersikkerhed.

Virksomheder har i årene op til 2018 været nødt til at sætte et større budget til side for at få styr på deres GDPR-compliance, og i den proces har de muligvis også generelt haft et større fokus på, hvordan virksomhedens IT skal håndteres. Eftersom GDPR måske er blevet "hverdag" kan det være, at IT-indsatsen er blevet mere afslappet, samt for hvert år der går bliver det lettere og billigere at udføre cyberangreb[77]. Tilgængeligheden for de værktøjer der kræves i forhold til at udføre et angreb, er blevet større, og derfor kan der være en stigning i antal cyberangreb.

[76] PwC Cybercrime Survey 2019, 2019
[77] Regeringen, 2018



[78]

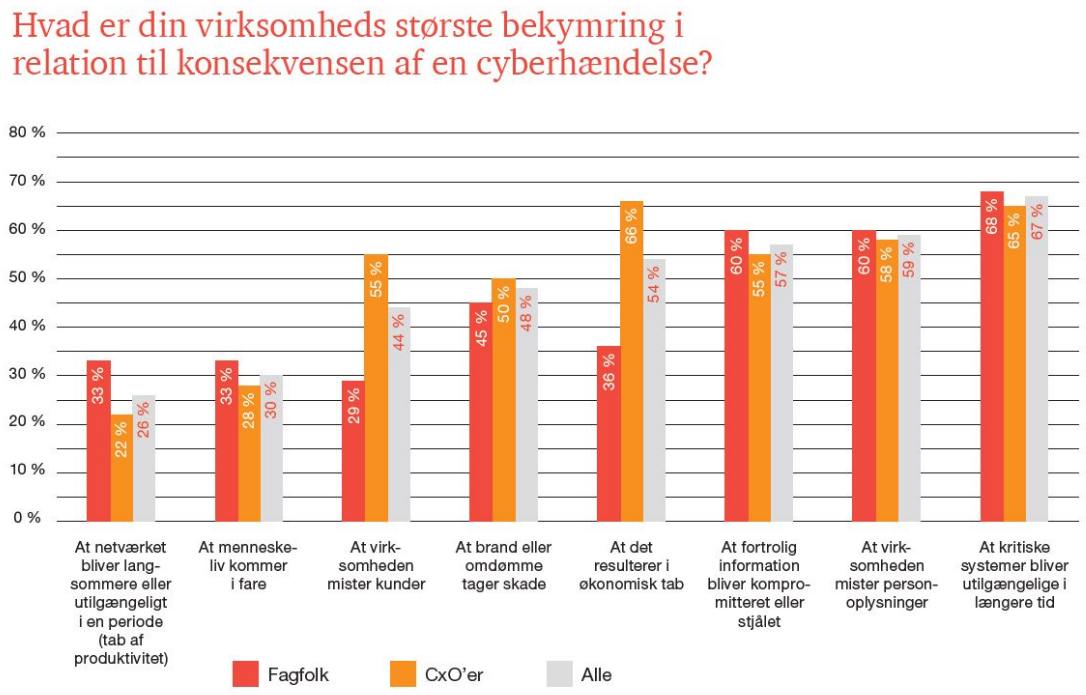
Jf. undersøgelsen er der en faldende tendens i bekymring om cybertrusler i forhold til 2015-2017, men en lille stigning fra 2018 til 2019. Denne stigning kan skyldes, at der har været et større fokus på cybersikkerhedsområdet og denne opmærksomhed kan medføre større bekymring om mulige angreb, fordi brugeren er blevet mere opmærksom. Bekymringen falder som nævnt i 2018, hvilket kan være fordi de adspurgte virksomheder har fået rigtig godt styr på deres cybersikkerhed i forlængelse af GDPR.

> *"Det er PwC's erfaring, at stigningen i antallet af sikkerhedshændelser og de skærpede regler til cybersikkerhed samt GDPR har gjort ledelsen mere opmærksom på cyber- og informationssikkerhedsrisici, hvilket kan have ført til de dedikerede budgetter."*[79]

Ydermere viser undersøgelsen, at der er et skel ift. bekymring om cybertrusler mellem fagfolk og CXO'er, hvor ledelsen bekymrer sig mere. Det kan skyldes, at de

[78] PwC Cybercrime Survey 2019, 2019
[79] PwC Cybercrime Survey 2019, 2019

to faggrupper prioriterer forskelligt. Undersøgelsen viser en stor forskel i, hvad de ser som den største trussel og hvilken påvirkning et angreb kan have, og dermed også hvor deres bekymringer ligger (se nedenstående figur).



80

Den største bekymring blandt fagfolk er, hvis der skulle ske noget med de kritiske systemer. Det kan skyldes, at fagfolk ser størst værdi i at vedligeholde de kritiske systemer. Dette ligger også højt på ledelsens bekymringer, men ledelsens største bekymring ligger derimod ved om et angreb kan føre til økonomisk tab. Bekymringen for at et angreb kan føre til økonomisk tab er meget forskellige ved fagfolk og ledelsen, samt ved om virksomheden kan miste kunder.

Erkendelsen af at cybersikkerhed er i konstant forandring og er noget som konstant skal holdes et vågent øje med, kan være med til at skabe den stigning, som man ser i 2019. Derfor gælder det for virksomheden om at have ledelsen med for at kunne

[80] PwC Cybercrime Survey 2019, 2019

sikre, at truslen bliver taget seriøst, men også sørge for at alle medarbejdere er opmærksomme på de trusler, der er i den digitale verden.

IT-budgetter

Med en stigning i antal virksomheder, der har oplevet et angreb samt en stigning i bekymring, viser PwC-undersøgelsen ligeledes en stigning i større virksomheders IT-budgetter. Dette kan være grundet den frygt der ligger bag et angreb, samt udspillet efter et angreb. Dette kan skyldes, at danske topchefer frygter ondsindede aktører mere end nogensinde, og derfor ser man en stigning i budgetterne[81].

> *"Det er ikke uden grund, at der især i de større virksomheder bliver investeret mange penge i cyber- og informationssikkerhed. 61 % af respondenterne fra de større virksomheder svarer nemlig, at de har været udsat for mindst én sikkerhedshændelse* […] *tallet er 33 % i de mindre virksomheder"*[82]

Større virksomheder > 200 medarbejdere[83]

År	Budget
2019	kr 19.000.000,00
2020	kr 20.500.000,00
Ændring i kr.	kr 1.500.000,00
Ændring %	7,89%

Stigningen i de større virksomheders budgetter er heller ikke uden grund, da de kan have en større vidensafdeling, og de kan derfor være mere attraktive mål for en ondsindede aktører.

[81] Mortensen, 2020
[82] PwC, Cybercrime Survey 2019, 2019
[83] PwC Cybercrime Survey 2019, 2019

> *"[...] de større virksomheder, der bliver udsat for flest målrettede sikkerhedshændelser. Her svarer 45 %, at de har været udsat for én eller flere målrettede sikkerhedshændelser, mens tallet er 29 % for de mindre virksomheder."*

De større virksomheder tager derfor truslen om cyberkriminalitet mere seriøst end de mindre virksomheder, og formentlig skyldes det, at de ved, at et angreb kan koste halve til hele milliarder at blive ramt af ondsindede aktører[84].

Mindre virksomheder <200 medarbejdere[85]

År	Budget
2019	kr 700.000,00
2020	kr 550.000,00
Ændring i kr.	-kr 150.000,00
Ændring %	-21,43%

I forhold til budgetterne for mindre virksomheder, viser PwC-undersøgelsen, at der sker et fald på over 20 % i deres IT-budgetter. Det kan skyldes, at de mindre virksomheder har haft et større budget for at kunne nå deres compliance i forhold til GDPR og derfor har haft et større budget op til.

> *"[...] 33 % i de mindre virksomheder, at de har været udsat for mindst én sikkerhedshændelse inden for det seneste regnskabsår, mens 29 % angiver, at de har oplevet én eller flere sikkerhedshændelser, der var målrettet deres virksomhed."*[86]

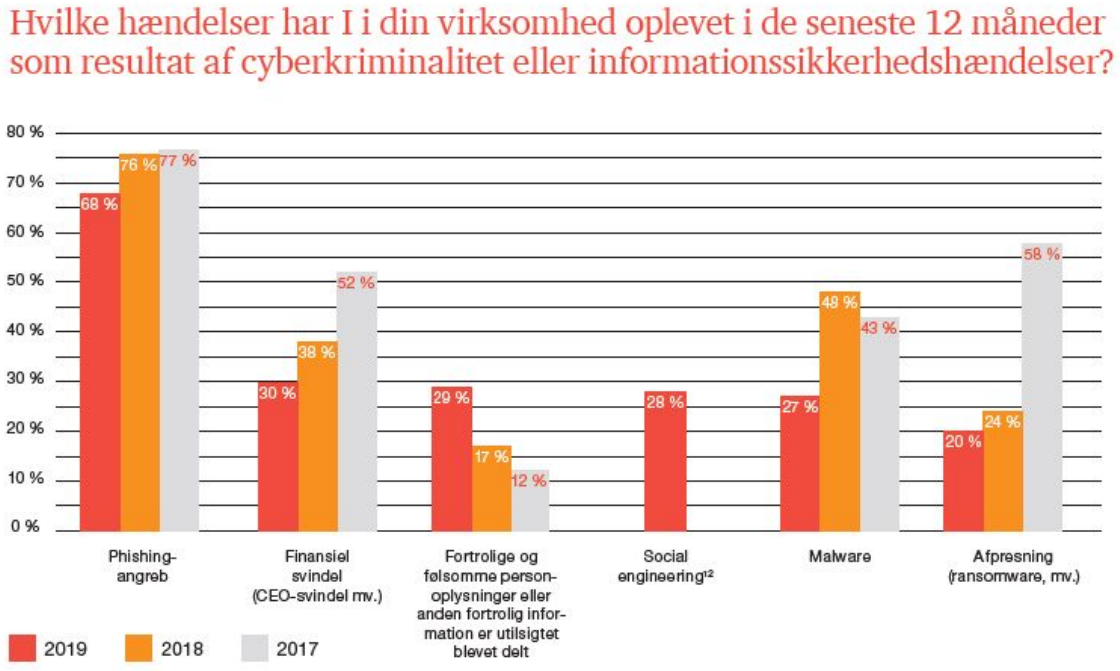
[84] Mortensen, 2020
[85] PwC, Cybercrime Survey 2019, 2019
[86] PwC, Cybercrime Survey 2019, 2019

Antallet af angreb mod de mindre virksomheder, om de har været udsat for én hændelse eller flere, er meget ens. Dette kan skyldes, at når der først er et svagt punkt i IT-systemet, kan det være med til at skabe flere hændelser.

Typer af angreb

PwC's Cybercrime Survey 2019 har delt angreb op i seks forskellige kategorier: 1) Phishing-angreb, 2) Finansiel svindel, 3) Fortrolige og følsomme personoplysninger eller anden fortrolig information er utilsigtet blevet delt, 4) Social engineering, 5) Malware og 6) Afpresning.

Som den helt store trussel ligger phishing-angreb klart i top. 68 % af virksomhederne har været udsat for et phishing-angreb inden for de seneste 12 måneder. Der er dog sket et fald siden 2018, hvor antallet var 76 % og i 2017 var det 77 %.



87

Faldet i antallet af phishing-angreb kan skyldes, at awareness træning har fået en større opbakning i virksomhederne og derfor er medarbejderne blevet bedre til at opdage, når det er en ondsindet aktør, der prøver at få adgang.

[87] PwC, Cybercrime Survey 2019, 2019

> *"58 % af respondenterne fra de større virksomheder, at medarbejderne testes i læringsmaterialet, mens tallet er lavere i de mindre virksomheder, hvor 48 % svarer, at medarbejderne testes."*[88]

Ved at teste medarbejderne løbende og lave awareness træning kan det være med til at skabe et arbejdsmiljø, hvor virksomhedens medarbejdere er opdateret på de trusler, der er og dermed også er i stand til bedre at agere i den digitale verden.

I grafen fra PwC's Cybercrime Survey 2019 er der kommet en ny post på i 2019, som omhandler social engineering. Social engineering er f.eks. en medarbejder bliver påvirket psykologisk af en ondsindet aktør til at udføre ting for personen. På den måde udfører den ondsindede aktør deres angreb via en medarbejder. I disse situationer er det ikke afpresning eller phishing men via en vis form for tricktyveri overbevises medarbejderen til at have tillid til den ondsindede aktør. I disse tilfælde er det vigtigt, at medarbejderne har gennemgået awareness træning, så de bedre kan bedømme, hvad der er et angreb og hvad der ikke er.
Både ved phishing og social engineering er problemet medarbejderne, og dermed er det de manuelle kontroller, som er problemet, da de kan blive påvirket af medarbejderne.

PwC's Cybercrime Survey 2019 giver et indblik i en verden, som normalt ikke er mulig at få indblik i. Den viser overordnet set, at der er et behov for at blive ved med at give cybersikkerhed et konstant fokus. Den digitale verden er i konstant forandring, og det er derfor afgørende for at sikre virksomhedernes fremtid at blive ved med at udvide awareness træninger for medarbejdere samt kontroller. Det er vigtigt at få hele virksomheden med på den forandring, der skal til for at håndtere cyberkriminalitet. Derfor er det specielt vigtigt at have ledelsen med ind i udarbejdelsen af virksomhedens IT-sikkerhed.

[88] PwC, Cybercrime Survey 2019, 2019

Fokuset skal derfor for fagfolkene være på at få identificeret trusler, for ledelsen at få kommunikeret problemerne om cyberkriminalitet ud og få medarbejderne til at forstå truslerne og dermed få skabt tillid til den cybersikkerhed, som virksomheden får skabt. For ledelsen er det ligeledes vigtigt at få skabt en balance mellem IT-budgetterne samt investeringer inden for IT og sørge for, at virksomheden er fremtidssikret inden for IT.

COVID-19 CFO Pulse Survey: Corona-krisens indflydelse på IT-sikkerhed[89]

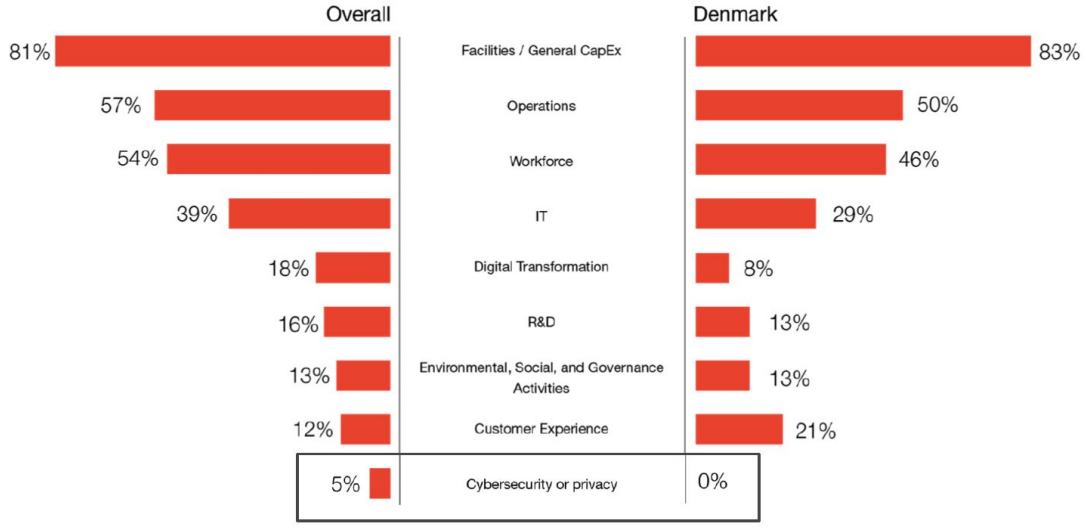
COVID-19 CFO Pulse Survey er også udført af PwC, men den undersøger blandt CFO'er deres prioriteringer i forbindelse med corona-udbruddet. På verdensplan er der blevet deltager 871 CFO'er fra 24 lande i undersøgelsen og heriblandt er 48 danske. Undersøgelsen kører hver anden uge i løbet af corona-krisen og den rapporterer om de tendenser, der er i de lande, hvor der minimum er kommet 30 besvarelser. CFO Pulse Survey giver et indblik i, hvad der foregår i CFO'ens verden under corona-krisen. Dermed giver undersøgelsen en idé om, hvad en krise gør ved virksomhederne ift. deres IT-sikkerhed.

Mere specifikt i forhold til cybersikkerhed giver undersøgelsen et indblik i, hvordan prioriteringen ligger med budgetterne og hvor de ser en mulig nedskæring i krisen og hvilke konsekvenser corona-krisen kan have.

Under krisen svare 21% af CFO'erne i undersøgelsen at cybersikkerheds risiko som den største bekymring, hvilket kan være grundet den støre mængde er hjemmearbejdene, samt at 73% af de danske CFO'er forventer et fald i omsætningen som følge af corona-virus.

[89] PwC, COVID-19 CFO Pulse Survey, 2020

Disse typer investeringer overvejes annulleret som et resultat af COVID 19



90

Som det fremgår af den ovenstående graf, ligger cybersikkerhed som en type investering, der overvejes annulleret på 5 % på det globale plan, mens den i Danmark ligger helt nede på 0 % Årsagen til dette kan være, at virksomhederne i Danmark ser behovet for at vedligeholde de allerede eksisterende programmer, som de har sat i værk mht. cybersikkerhed, i en krisetid. Det er derfor ikke en investering, hvor de danske virksomheder vil stoppe de allerede eksisterende opgaver, der ligger i pipeline. Jf. undersøgelsen må man da forvente, at de danske virksomheder fortsætter med de projekter, der allerede er i gang.

Corona-krisen er kendetegnet ved, at medarbejdere skal blive hjemme, og derfor kommer der et væld af trusler ved at arbejde hjemmefra. Når den fysiske kontakt mellem medarbejdere forsvinder, kan det skabe en usikkerhed i forhold til, hvem medarbejderen egentlig er i kontakt med.
Når medarbejderne arbejder hjemmefra, kommer der til at være en større kommunikation via mail, videosamtaleprogrammer og lignende. Det skaber flere

[90] PwC, Cybercrime Survey 2019, 2019

muligheder for, at virksomhederne kan blive angrebet via phishings links. De manuelle kontroller er derfor sat under et pres for at blive automatiseret for at fjerne truslen ved phishing angreb eller lignende.

Hjemmearbejdspladsen er en god løsning til at holde hjulene i gang under corona-krisen, men den kommer ikke uden problemer. Virksomheder, som ikke har fået etableret remote access til deres medarbejder inden krisen, eller som simpelthen ikke har stor nok kapacitet på deres netværk, kan opleve, at corona-krisen har skabt et problem, som skulle løses med det samme. Det kan medføre, at virksomheden ikke har styr på oplæring af medarbejdere, og det kan gøre virksomhederne sårbare overfor cyberangreb.

Webinar: Cybersecurity-udfordringer i krisetider[91]

Som nævnt i metodeafsnittet, stillede jeg spørgsmål til værterne ved PwC's webinar omhandlende cybersecurity-udfordringer i krisetider. Mit spørgsmål gik på: "*Hvordan påvirker corona-krisen tilliden til de interne kontroller?*" (se Bilag 1 for transskription af besvarelserne på spørgsmålet).

Spørgsmålet blev stillet for at eksperternes syn på påvirkningen af kontrollerne som følge af en krise. Natasha Lembke, partner og Head of Finance Transformation i PwC svarede blandt andet:

> *"Det vil komme an på, om man har manuelle interne kontroller, som er meget manuelt funderet, så vil tilliden til det helt sikkert falde.* [...] *Det vil komme an på, om man har manuelle interne kontroller, som er meget manuelt funderet, så vil tilliden til det helt sikkert falde."*[92]

Udfordringerne der kommer ud fra at de manuelle kontroller vil blive udsat kan have større konsekvenser for hele virksomheden. Et allerede udsat del af kontrollerne vil

[91] PwC, Cybersecurity-udfordringer i krisetider, 2020
[92] PwC, Cybersecurity-udfordringer i krisetider, 2020

blive udsat for et endnu større pres, og det kan være med til skabe muligheder for ondsindede aktører. Den tillid, som virksomhederne ligger i deres kontroller, er kritisk for, at revisor kan få et billede af virksomheden og dermed udføre sit arbejde med høj sikkerhed. Natasha Lembke siger også:

> *"Men hvis man har automatiske og mere indbyggede kontroller i systemerne, så har vi ikke jf. de dialoger jeg har haft med kunder, ikke en forventning om, at det bliver ændret."*[93]

Et automatisering af kontrollerne kan derfor være med til at sikre virksomheden og dermed skabe større tillid til dens kontroller. Dertil siger Mads Nørgaard Madsen, partner og Head of Security i PwC i webinaret:

> *"I forvejen var den (red. interne kontroller) måske ikke høj nok mange steder, og nu bliver den endnu mere udsat."*[94]

Corona-krisen sætter pres på allerede udsatte kontroller og de virksomheder, som inden krisen ikke havde sikret sig vil derfor blive mere udsat. Virksomheder skal tænke fremad og forberede sig på de ændringer, der kommer og automatisering kan være en mulig løsning. Her nævner Mads Nørgaard Madsen:

> *"Det pres, der er kommet med COVID-19 sætter et enormt pres på hele digitaliseringsagendaen."*[95]

Mange virksomheder har derfor under corona-krisen set nødvendigheden i at opruste virksomheden til hvad der måtte komme i fremtiden. Om hjemmearbejdspladsen bliver en mere fast løsning, vides ikke, men virksomheder

[93] PwC, Cybersecurity-udfordringer i krisetider, 2020
[94] PwC, Cybersecurity-udfordringer i krisetider, 2020
[95] PwC, Cybersecurity-udfordringer i krisetider, 2020

skal forberede sig på, at det kan være en mulig løsning, hvis der kommer lignende situationer.

De to eksperter nævner også, at IT-sikkerhed bliver "brand defining"[96], og at det er en trend, som de har set igennem de seneste år. Det betyder, at det bliver brugt aktivt i kommunikation både til brugere, andre virksomheder og i forbindelse med tiltrækning af nye medarbejdere.

"Derfor skal jeg også have tillid til, at din sikkerhed (red. en anden virksomhed) lige så vel som at min sikkerhed også skal være i orden." Natasha Lembke

Som antyder i indledningen er tillid afgørende ift. samarbejder mellem virksomheder. Ved at få de rette revisionserklæringer kan virksomheden vise, at de er en troværdig partner at samarbejde med og at deres IT-sikkerhed, om det er under krise eller ej, ikke fejler noget. Det er blandt andet derfor op til revisorer at sikre at deres erklæringer giver et godt billede af en virksomhedens IT-sikkerhed.

Gartner CIO Survey[97]: Finanskrisen

Årsagen til at denne undersøgelsen er taget er for at give indblik i IT-budgettering i forbindelse med kriser. Undersøgelsen er lavet i 2009 og giver et billede på budgetter og hvordan CIO's agerede efter Finanskrisen i 2008.CIO-undersøgelsen er baseret på mere end 1.500 besvarelser, som er indsamlet fra september til december 2008.

Resultaterne af Gartner CIO Survey fra 2009 viser, at de globale kommercielle og offentlige IT-budgetter havde en flad til beskeden stigning på 0,16 % fra 2008-2009. I forhold den finansielle nedgang generelt på markedet efter Finanskrisen, ser man

[96] PwC, Cybersecurity-udfordringer i krisetider, 2020
[97] Gartner, 2009

ikke et større fald i IT-budgetterne og undersøgelsen viste, at det gennemsnitlige IT-budget for 2009 var fladt.

Undersøgelsen fremhæver, at IT-området siden 2003 har haft en beskeden vækst og fra 2004-2009 har haft en vækst på 2,5 %. Dette kan være med til, at budgetter har ligget på passende niveau inden for området og der simpelthen ikke var mulighed eller behov for at mindske det.

> *"CIOs report that business expectations of IT are concentrating more on changing the enterprises cost structure through business process, workforce and organizational change, than just running IT."*[98]

Behovet for at have solide IT-systemer til at kunne optimere arbejdsindsatsen er derfor meget lig det, man ser i dag. Problemet med, at IT-budgettet ikke stiger, er at CIO enten må vælge nogle billigere løsninger eller lave nogle nedskæringer på allerede etablerede løsninger, og derfor er der ingen vækst Undersøgelsen oplyser dog ikke, om der er et dedikeret budget til cybersikkerhed, men ud fra den information Gartner CIO Survey giver, må jeg gå ud fra, at cybersikkerhed ligger under selve IT-budgettet.

De udfordringer, som virksomhederne stod overfor i Finanskrisen, er lignende det, man ser i dag, hvor der er en nedgang på det finansielle marked. Det er et ustabilt marked, hvor ting kan ændre sig meget hurtigt og man må derfor gå ud fra, at ledelsen rundt om i virksomhederne konstant prøver at afbalancere budgetter efter de indtægter og omkostninger, de har. Generelt så man under Finanskrisen en nedgang i budgetterne.

[98] Gartner, 2009

Rasmus Madsen Carlslund
Cand.merc.aud.
Den 31. maj 2020

Diskussion

I følgende afsnit diskuterer dette speciale, hvordan revisor sikrer sig, at virksomhederne lever op til de krav, der er til cybersikkerhed, så de sikkert kan agere i den konstant udviklende digitale verden. Diskussionen tager udgangspunkt i det analyserede og svarer derfor på underspørgsmålene:

- ➔ **Underspørgsmål 1:** Hvordan håndteres truslen om cyberkriminalitet blandt de danske virksomheder generelt?
- ➔ **Underspørgsmål 2:** Hvordan påvirker corona-krisen cyberkriminalitet og virksomhedernes IT-sikkerhed, og hvordan kan virksomhederne håndtere krisen?

ISAE 3000[99], ISAE 3402[100] samt ISRS 4400[101]

Revisor er offentlighedens tillidsrepræsentant og har derfor en vigtig rolle, når det kommer til at sikre virksomheder og give en uafhængig erklæring vedrørende cybersikkerhed. Revisoren har nogle vejledninger og standarder, som kan bruges til at sikre, at virksomhederne får de rette erklæringer. I dette speciale kigger jeg som bekendt på ISAE 3000, ISAE 3402 samt ISRS 4400.

De tre standarder kan bruges til forskellige handlinger, og det er derfor vigtigt for revisoren at vide, hvornår hvilke standarder skal tages i brug og finde det rette serviceniveau til den pågældende virksomhed. I nedenstående gennemgås de tre standarder, som benyttes ift. sikring af IT-sikkerhed.

[99] ISAE 3000
[100] ISAE 3402
[101] ISRS 4400

ISAE 3000 bruges til at aftale de specifikke revisionshandlinger, som bliver udført. Dette kan foregå efter f.eks. skabelonen udført at FSR's Cybersikkerhedsudvalg. ISAE 3000 tjekker kun specifikke områder, og der gives derfor kun en konklusion fra revisor ud fra de kriterier, der er defineret i erklæringen. Den kan derfor bruges til at sikre bestemte områder for virksomheden som f.eks. GDPR og kan derfor være en kosteffektiv måde for virksomheden at sikre de mest nødvendige områder inden for cybersikkerhed. At beskytte persondata kan være et større foretagende, og derfor det både for virksomhedens ledelse men også virksomhedens samarbejdspartnere være en sikring, at databehandleren har en betryggende behandling af de personoplysninger, som den dataansvarlige er ansvarlig for.

ISAE 3402 bruges til at få et overblik over virksomhedens systemer, som påvirker relevante forhold i forhold til regnskabsaflæggelse, hvor kontrollerne ligger hos en outsourcing-leverandør. Dette sker ved at opsætte en række kontrolmål, kontrolaktiviteter samt tests. Ved at lave en gennemgang af virksomheden kan revisor tage udgangspunkt i den certificering, som er relevant. Det kunne f.eks. være ISO 27001/2, CobiT eller lignende. ISAE 3402 er derfor med til at skabe tillid mellem virksomheder og kan stå som en sikkerhed blandt samarbejdspartnere i forhold til at sikre, at samarbejdspartnerens cybersikkerhed er i orden.

ISRS 4400 bruges, når revisor har et højt vidensniveau om de ydelser og kontroller, som virksomheder har. Den kan derfor i flere tilfælde være mere effektiv i forhold til at lave en gennemgang af virksomheder og dens aktiviteter i forhold til cybersikkerhed. Til forskel for ISAE 3000 og ISAE 3402 giver ISRS 4400 ikke den endelige konklusion over revisors arbejder. Det overlades i stedet til modtager at konkludere på arbejdshandlingerne.

Ved brug af revisionserklæringer kan revisor sikre, at IT i virksomheder bliver håndteret på en korrekt og fornuftig måde især ved brug af en outsourcing-leverandører. Revisor skal bruge den information til at sikre, at udførelsen af den

finansielle revision kan ske med en høj grad af sikkerhed, og at revisors konklusion derfor har en høj grad af troværdighed.

Cybersikkerhed påvirker hele virksomheden, og derfor påvirker den også revisors effektivitet ved udførelsen af revision. I og med at den digitale verden er i konstant forandring kan det være en stor opgave for revisor at sikre, at en virksomhed har de nødvendige kontroller og cybersikkerhed. Revisor kan derfor ved udførelsen af sine erklæringer samtidigt have en mere rådgivende rolle overfor virksomheden, hvor han hjælper dem til bedre at navigere og identificere de risici, der er.

Revisor skal konstant opdatere sig

Det er vigtigt, at revisoren holder sig opdateret på cyberkriminaliteten, så revisor kan yde den rigtige og opdaterede rådgivning ved at følge de korrekte standarder og holde sig opdateret. I situationer hvor revisor ikke har den rette viden eller har en mangelfuld viden, er det vigtigt, at revisor søger hjælp andetsted fra i form af eksperter indenfor det område, hvor revisoren efterlyser viden.

Fordi cyberkriminalitet er et område, hvor der sker en konstant udvikling, kan det kræve meget af revisor ift. at være helt opdateret. Derfor kan det diskuteres, hvorvidt mindre revisionsselskaber har de nødvendige ressourcer samt viden til at kunne udføre opgaver indenfor IT-revision for større virksomheder, medmindre disse mindre revisionsfirmaer specialiserer sig indenfor netop IT-revision. Af den årsag kunne man forestille sig, at opgaven også i fremtiden bliver overladt til “the big 5”. De har en udvidet adgang til en større kundegruppe og dermed større mulighed for at tilegne sig viden. De kan bruge den viden de opnår ved een kunde på resten af kundebasen. Ligesom virksomheder kan det være brand defining for revisorhuse, at de har de rette redskaber og opdateret viden til at kunne udføre opgaver indenfor IT-revision på det rette niveau.

Diskrepans mellem opfattet virkelighed og faktisk virkelighed

Som nævnt i analysen af Cybercrime Survey 2019 mener en stor andel, at de er beskyttet mod cyberangreb. På den anden side ser vi, at en stor andel (51 %) af de adspurgte inden for de seneste fem år har haft en hændelse. Det kan betyde, at virksomhederne tror, at de er beskyttet men måske ikke har identificeret truslen endnu og dermed ikke er helt så forberedte, som de måske selv tror. På den måde kan der være en forskel mellem virksomhedernes egne opfattelser af deres IT-sikkerhed og den faktiske realitet.

Omvendt kan det også være, at den halvdel af de adspurgte, som mener, at de har styr på deres IT-sikkerhed netop er den gruppe, som ikke er blevet angrebet er cyberkriminelle.

Som forsvarsminister Trine Bramsen nævner, er der formentlig et stort skyggetal ift. cyberangreb der ikke bliver indberettet, fordi det er pinligt[102]. Derfor kan det diskuteres, hvad de reelle tal for cyberangreb faktisk er. Dog er PwC's undersøgelse, Cybercrime Survey 2019, anonym og derfor må man forvente, at den er pålidelig. Ydermere er det specialets opfattelse, at undersøgelsen viser et repræsentativt udsnit af det danske erhvervsliv.
Den digitale verden er i konstant forandring og ved at der er flere og flere sårbarheder i virksomhederne, er det vigtigt for virksomhederne at indse og erkende, hvis deres virksomhed ikke har de rette foranstaltninger ift. IT-sikkerhed, så problemet kan blive håndteret. Det kan diskuteres om virksomhederne også synes, at det er pinligt, hvis deres IT-sikkerhed ikke er god nok og derfor ikke har lyst til at få professionel hjælp.

[102] Bramsen, 2020

Mindre virksomheder nedsætter IT-budgetter, mens større virksomheder hæver budgetterne

Man ser en nedgang i IT-budgetterne for de mindre virksomheder[103]. Det kan måske skyldes, at deres mentalitet er, at nu har de brugt en del penge på det her IT og nu er det sikret i den kommende fremtid. Men virkeligheden er bare en anden, da ondsindede aktører konstant leder efter nye muligheder at angribe på. Derfor bliver en virksomhed aldrig "færdig" med at investere i IT-sikkerhed. Derfor er det vigtigt, at virksomhedens interne kontroller samt den sikkerhed de får fra en outsourcing-leverandør lever op til de krav og standarder, der er.

Problemet ift. at investere i IT-sikkerhed er størst i de mindre virksomheder til forskel fra de større virksomheder, hvor budgetterne sættes op og cybersikkerheden står højt på dagsordenen.

Hvis argumentet blandt de mindre virksomheder er, at de ikke har råd til at prioritere IT-sikkerhed, må spørgsmålet fra revisor være: "*Har virksomheden råd til at lade være med at prioritere cybersikkerhed?*" Det kommer blandt andet an på typen af virksomhed og produkt, men f.eks. GDPR gælder for alle virksomheder og kan være en dyr lærestreg at få.

Kan virksomheden stole på sine kontroller, hvis IT-budgetterne sænkes?

Det drejer sig ikke kun omkring at beskytte virksomhedens data, men også om at sikre at virksomheden har en vis integritet i dens kontroller. Ved at nedsætte budgetterne kan det føre til at den sikkerhed og tillid, som virksomheden har til sine kontroller vil blive mindsket. Det kan også betyde, at revisor ikke kan udføre sit arbejde med en høj grad af sikkerhed og dermed ikke kan afgive en konklusion. Det

[103] PwC, Cybercrime Survey 2019, 2019

kan være en glidebane for virksomheden, som kan lede til lovbrud (f.eks. GDPR) og i sidste ende kan have en effekt på going concern.

Medarbejdere er den største trussel, men også et stærkt forsvar

De virksomheder, som i dag har nogle stærke sikkerhedsforanstaltninger sat op, skal fortsat være opmærksomme, da deres medarbejdere kan være deres største trussel ift. cyberangreb.

Det kan være svært at sikre sig imod f.eks. social engineering, og det kræver, at medarbejderen selv kan være med til at identificere en trussel. Derfor skal revisor under sin undersøgelse af virksomheden være opmærksom på, om virksomheden har den rette IT-ledelsesstruktur og at virksomheden har en god IT-skik. En god IT-ledelsesstruktur og en generelt god IT-skik blandt ledelse og medarbejderne kan betyde, at de ledelse og medarbejdere bliver et stærkt værn mod cyberangreb. Derfor er det vigtig, at virksomheden har nogle strukturer, awareness træning eller vejledninger til deres medarbejder, så de selv kan identificere trusler og dermed agere mere sikkert i den digital verden. At man har den korrekte og kontinuerlig awareness træning er med til at sikre dygtige medarbejdere, som står klar, når de IT-kriminelle slår til.

Corona-krisen

> "*Vi skal hellere handle i dag, end fortryde i morgen.*" [104]

Sådan lød det, da statsminister, Mette Frederiksen den 11. marts 2020 lukkede Danmark ned i forbindelse med, hvad der senere betegnes som corona-krisen. Alle private virksomheder blev på det kraftigste opfordret til, at deres medarbejdere skulle arbejde hjemmefra, og med ét blev hele aktivitetsbilledet ændret. Det var her virksomhedernes IT-ledelse, -systemer samt -sikkerhed blev sat på prøve. Nogle

[104] Frederiksen, 2020

virksomheder kunne håndtere det store pres som der pludseligt på deres IT-setup og -sikkerhed, mens andre stod måbende og gik en presset periode i møde.

Corona-krisen påvirker cyberkriminalitet og virksomhedernes IT-sikkerhed, fordi krisen sætter pres på de allerede eksisterende kontroller. De virksomheder, som ikke har en ordentligt IT-strategi og -system udsættes for en omvæltning af deres arbejdsgange.

Man kan formode, at krisen har givet meget læring til virksomhederne, da de har skulle agere agilt og indrette sig lynhurtigt efter den nye situation.

Fremtidens IT-sikkerhed

Måske man ser en ny hverdag, hvor det er langt mere almindeligt, at virksomhedernes medarbejdere arbejder hjemmefra som en mere fast løsning. Det betyder, at virksomhederne skal sikre deres IT-sikkerhed og -systemer, så de kan håndtere dette pres. Revisoren kan være med til at sikre, at virksomhedens data og arbejdshandlinger bliver håndteret korrekt, hvis virksomheden vælger en outsourcing leverandør til at håndtere deres IT-sikkerhed.

Med det yderligere pres på de manuelle kontroller, som der er som følge af corona-krisen, vil der formentlig i fremtiden ske en større automatisering af virksomhedernes kontroller som et værn med de sårbarheder, der er ved de manuelle kontroller. Dermed mindsker virksomhederne det pres, der er på de manuelle kontroller.

I PwC's COVID-19 Pulse Survey kan man se, at de cybersikkerhedsprojekter, der allerede ligger i pipeline, ikke bliver annulleret under krisen[105]. Det må betyde, at der er en prioritering af cybersikkerhed. Selvom virksomhederne skærer ned på flere

[105] PwC, COVID-19 CFO Pulse Survey, 2020

andre punkter, bliver det fortsat prioriteret at udvikle på virksomhedernes cybersikkerhed.

Virksomheder, der ikke har arbejdet intensivt med IT-strategi og -sikkerhed vil formentlig inden for det næste stykke tid indse, at de skal ændre deres arbejde med IT-sikkerhed og -systemer - hvis de da ikke allerede har valgt at ændre deres prioriteringer. Hvis der kommer en lignende krise i fremtiden skal virksomhederne være i stand til hurtigt at kunne ændre deres arbejdsgange til at passe det behov, der er. De skal være mere agile overfor pludselige forandringer i det digitale marked.

Et tilbageblik på Finanskrisen

Ved at kigge tilbage på Finanskrisen i 2008, ser man en lignende tendens. Her blev IT-budgetterne ikke sat ned, men holdte sig fladt efter en ellers svær økonomisk tid. Man kan gisne om, at corona-krisen enten vil gennemgå en lignende proces eller stige grundet erkendelsen af, at IT er en vital del af virksomhedens arbejdsgang.
Omvendt har man ikke set slutningen på corona-krisen og ved derfor ikke, om den økonomiske situation kommer til at være endnu værre, end den man så i forbindelse med Finanskrisen i 2008. Helt generelt kender man ikke omfanget af corona-krisen både ift. økonomi og IT-sikkerhed.

Fremtiden for revisoren

Grundet den større automatisering som revisionsfaget gennemgår, vil revisors arbejde ift. at sikre virksomheder i deres arbejde med IT være mere relevant i fremtiden. De klassiske opgaver vil muligvis forsvinde, og derfor kan revisors rolle bliver mere rådgivende. Det er derfor vigtigt at revisor er agil overfor de nye roller, der kommer i fremtiden. Det formodes, at revisors rolle bevæger sig mere væk fra standardisering og over i en mere værdiskabende rolle. Som Sumit Sudan, partner og senior manager i Deloitte formulerer det:

"*Jeg håber dog, at vi er i stand til at flytte os fra det mere standardiserede arbejde til mere værdiskabende arbejde, hvor man ikke lige kan få en robot til at overtage – altså områder der kræver menneskelig indsigt, "touch" og forståelse.*"[106]

[106] Sudan, 2017

Rasmus Madsen Carlslund
Cand.merc.aud.
Den 31. maj 2020

Konklusion

Formålet med dette speciale er at svare på den følgende problemformulering: *Hvordan sikrer revisorer sig, at virksomhederne lever op til de krav, der er til cybersikkerhed, så de sikkert kan agere i den konstant udviklende digitale verden?*

Den overordnede problemformulering bliver besvaret ved at udfolde fænomenerne cyberkriminalitet og IT-sikkerhed ved at besvare på de to underspørgsmål. 1) *Hvordan håndteres truslen om cyberkriminalitet blandt de danske virksomheder generelt?* og 2) *Hvordan påvirker corona-krisen cyberkriminalitet og virksomhedernes IT-sikkerhed, og hvordan kan virksomhederne håndtere krisen?*

Nationalt fokus på cybersikkerhed

Der er en grund til, at selveste forsvarsministeren italesætter udfordringer med cybersikkerhed: Det er afgørende for det danske erhvervsliv at stå stærkt digitalt, fordi digitalisering er fremtiden. På baggrund af den nationale cybersikkerhedsstrategi[107] konkluderes det, at det er i nationens interesse, at de danske virksomheder kan agere sikkert i den digitale verden - dette gælder især de offentlige og samfundskritiske sektorer. Denne prioritering ses også hos FSR med udviklingen af Cybersikkerhedsrådet[108] og vejledninger, der går tilbage til 1989.

Revisors erklæringer

Det konkluderes, at revisor kan tage flere redskaber i brug for at kunne sikre, at virksomheder lever op til kravene, så de kan agere sikkert i den digitale verden. Revisor kan i samarbejde med virksomheder og deres outsourcing leverandører få lavet erklæringer, som er med til at sikre, at virksomhederne har de nødvendige

[107] Regeringen, 2018
[108] Det Kriminalpræventive Råd, 2020

foranstaltninger. I specialet bliver det konkluderet, at de mest anvendelige erklæringer i forhold til IT-sikkerhed er: ISAE 3000, ISAE 3402 samt ISRS 4400.

De erklæringer, revisor udfører, kan være med til at sikre virksomheden og deres samarbejdspartnere. Det er her kontrolarbejdet ligger, og her der laves en undersøgelse af virksomhedens nuværende aftaler samt kontrolområder i virksomheden og hos outsourcing leverandør. God IT-skik involverer også virksomhedens samarbejdspartnere ift. den data, virksomheden er ansvarlig for.

Revisor kan rådgive ud over erklæringerne i forbindelse IT-sikkerhed. Erklæringerne vil ikke dække hele virksomheden og revisor kan rådgive ift. de mangler, han eventuelt opdager under udførelsen af sine erklæringer. Følgende afsnit tager udgangspunkt i revisors rådgivning udover den han yder i forbindelse med erklæringerne.

Danske virksomheders generelle håndtering af cybersikkerhed

Nedenstående besvarer underspørgsmål 1 i forhold til, hvordan truslen om cyberkriminalitet håndteres af danske virksomheder generelt.

Der er generelt forskel på, hvordan større og mindre virksomheder håndterer cybersikkerhed. Man ser et fald i budgetterne i de mindre virksomheder, hvor de større virksomheder derimod sætter deres budgetter op. De større virksomheder opruster deres systemer indenfor cybersikkerhed og investerer dermed i IT-sikkerhed.

Det konkluderes, at virksomhederne kan have svært ved at have tillid til deres IT-kontroller, hvis de sænker deres IT-budgetter. Brug af IT kræver konstant opmærksomhed for at kunne være agil i den konstant foranderlige digitale verden. Det er ikke blot IT-systemerne, der skal være opdaterede, men også de medarbejdere, der benytter sig af dem. De er nemlig den største trussel, men også

et stærkt forsvar, hvis de er trænede og har en god IT-skik. Det gælder også revisor, som selvfølgelig skal have de rette kompetencer for at kunne fuldføre sine opgaver.

Det konkluderes, at der kan være en diskrepans mellem virksomheders opfattelse af deres egen IT-sikkerhed samt den realitet, der er. Det kan være fordi, de ikke har indsigten til at gennemskue deres IT-sikkerhed og/eller at de ikke ønsker at erkende, at der er et problem.

Danske virksomheders specifikke håndtering af cybersikkerhed ift. corona-krisen

Nedenstående besvarer underspørgsmål 2 i forhold til, hvordan corona-krisen påvirker cyberkriminalitet og virksomhedernes IT-sikkerhed.

Som følge af corona-krisen stiger presset på virksomhedernes cybersikkerhed, blandt andet i takt med at mange flere arbejder hjemmefra, og dermed skabes der flere sårbarheder i IT-sikkerheden. Formentlig netop fordi der er flere sårbarheder, oplever virksomhederne flere angreb på deres IT under corona-krisen. Krisen påvirker de interne kontroller i virksomheden og især de manuelle kontroller bliver udsat og er under pres.

Derudover ser man at cybersikkerhedsprojekter forbliver som planlagt før krisen, selvom det er en hård økonomisk periode for mange virksomheder. Årsagen til, at der fortsat investeres i IT-sikkerhed, kan hænge sammen med, at virksomheder har set nytteværdien af et sikkert IT-system, især under denne krisetid. Der konkluderes, at denne tilgang til IT-sikkerhed er meget lig den, man oplevede efter Finanskrisen, og derfor konkluderes det også, at IT-sikkerhed er essentielt for mange virksomheder, selvom økonomien er påvirket. Dertil skal det nævnes, at man ikke kender til corona-krisens endelige omfang økonomisk og ift. IT-sikkerhed.

Rasmus Madsen Carlslund
Cand.merc.aud.
Den 31. maj 2020

Fremtidens IT-sikkerhed

Corona-krisen har gjort IT-sikkerhedsbranchen en mulig tjeneste i den forstand, at den har sat et gyldent eksempel op, som viser, at man altid skal være klar på ændringer. Der er ikke nogen, der foreløbigt kommer til at glemme, da Danmark "lukkede ned". Derfor vil corona-krisen formentlig være det eksempel, som revisor tager frem, når han skal argumentere for vigtigheden af IT-sikkerhed. Det understreger, at virksomhederne aldrig ved, hvornår de pludseligt ville ønske, at de havde en stabil og kontinuerlig IT-sikkerhed og en generel god IT-skik, hvor medarbejderne har den rette træning til at træffe de rigtige valg, når det rigtigt gælder.

Det er et konstant kapløb med tiden, inden det næste store angreb eller den næste krise rammer. Det er derfor ikke kun at sikre sig mod de trusler, man ser i dag, men også være agil ift. hurtigt at tilpasse virksomhedens IT-sikkerhed til de nye udfordringer, som opstår. I dag kan en virksomheds IT-sikkerhed være komplet, men i morgen kan der være nye trusler, man ikke kender til i dag, og revisor kan være med til at hjælpe virksomheder til at opnå en høj grad af sikkerhed.

Derfor håber jeg som kommende revisor, at den læring, som virksomhederne tager med sig fra corona-krisen, er:

> "*Vi skal hellere handle i dag, end at fortryde i morgen*"[109].

[109] Frederiksen, 2020

Rasmus Madsen Carlslund
Cand.merc.aud.
Den 31. maj 2020

Litteraturliste

Berthing, H. H., Mogensen, J. K., Lind, B., Gotfredsen, K., Joensen, T. B., Mikkelsen, N. T., & Nielsen, F. S, 2011. *God IT Skik*.

Bramsen, T., 2020. *Et kapløb med tiden*. CXO I Magasinet, 23. udgivelse, s. 14-19. Hentet den 20. april fra: https://www.pwc.dk/da/publikationer/2020/pwc-cxo-magasinet-23.pdf

Bryman, A., 2012. *Social Research Methods*. 4. edition, Oxford: Oxford University Press

Det Kriminalpræventive Råd, 2020. Cybercrime - Det Kriminalpræventive råd. blev hentet maj 30, 2020 fra https://www.dkr.dk/media/9820/cybercrimefolder2018.pdf

EU Direktiv, 2006 (2006, maj 17). DIRECTIVE 2006/43/EC OF THE EUROPEAN ... - IAS Plus. blev hentet maj 30, 2020 fra http://www.iasplus.com/europe/0606auditdirective.pdf

Frederiksen, M., 2020. *Situationen kommer til at stille kæmpe krav til os alle sammen*. Pressemøde om corona-virus den 11. marts 2020. Hentet den 18. maj fra https://www.regeringen.dk/nyheder/2020/statsminister-mette-frederiksens-indledning-paa-pressemoede-i-statsministeriet-om-corona-virus-den-11-marts-2020/

Gartner, 2009. *How could IT budgets be flat in tough economic times?* Blev udgivet den 13. januar 2009. Blev hentet den 14. april fra: https://blogs.gartner.com/mark-mcdonald/2009/01/13/how-could-it-budgets-be-flat-in-tough-economic-times/

Hestbech, A., 2020. *Risikoen for cyberangreb lurer i dit hjemmekontor*. Blev hentet den 6. marts 2020 fra https://finans.dk/debat/ECE12051347/risikoen-for-cyberangreb-lurer-i-dit-hjemmekontor/?ctxref=ext

Højbjerg, H., 2009. *Hermeneutik, forståelse og fortolkning i samfundsvidenskaberne*. 2. edition: Roskilde Universitetsforlag

ISAE 3000 Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger , blev hentet maj 30, 2020 fra https://pro-karnovgroup-dk.zorac.aub.aau.dk/document/7000758092/1

ISAE 3402 Erklæringsopgaver med sikkerhed om kontroller hos en serviceleverandør, blev hentet maj 30, 2020 fra https://pro-karnovgroup-dk.zorac.aub.aau.dk/document/7000758094/1

ISRS 4400 Aftalte arbejdshandlinger vedrørende regnskabsmæssige oplysninger og yderligere krav ifølge dansk revisorlovgivning, blev hentet maj 30, 2020 fra https://pro-karnovgroup-dk.zorac.aub.aau.dk/document/7000758096/

Juul, S., 2012. *Samfundsvidenskabernes videnskabsteori: En indføring*. 1. edition: Hans Reitzels Forlag

Kuada, J., 2014. *Research Methodology. A Project Guide for University Students*. 1. edition, 2. oplag: Samfundslitteratur

Kvale, S. & Brinkmann S., 2015. *InterViews*. 1. edition ed. Los Angeles: Sage

Mogensen, J. K., 2018: *Revisors erklæringer om cybersikkerhed og persondatasikkerhed*. Udgivet i RR den 2. maj 2018. Blev hentet via Karnov den 14. marts 2020: https://pro-karnovgroup-dk.zorac.aub.aau.dk/document/7000820102/1?frt=cobit&hide_flash=1&page=1&rank=2#RR2018050014_20180502094021_1

Mortensen, S. W., 2020: *Danske topchefer frygter hackere mere end nogensinde*. Udgivet på Finans.dk den 5. marts 2020. Blev hentet den 6. marts 2020 fra https://finans.dk/tech/ECE11986124/danske-topchefer-frygter-hackere-mere-end-nogensinde/?ctxref=ext

Politico EU 2020(2020, marts 18). Brussels in talks with Netflix about reducing ... - Politico EU. blev hentet maj 30, 2020 fra https://www.politico.eu/article/brussels-in-talks-with-netflix-about-reducing-internet-congestion/

PwC, COVID-19 CFO Pulse Survey, maj 2020. *COVID-19 CFO Pulse Survey*. Blev hentet den 5. maj fra https://www.pwc.dk/da/covid-19/cfo-pulse-survey.html

PwC, Cybercrime Survey 2019, 2019. *Cybercrime Survey 2019*. Blev hentet den 16. december, 2019 fra https://www.pwc.dk/da/publikationer/2019/11/cybercrime-survey-2019.html

PwC, Cybersecurity-udfordringer i krisetider, 2020: *Cybersecurity-udfordringer i krisetider*. Webinar blev sendt live den 14. maj 2020. Blev hentet den 15. maj fra https://www.youtube.com/watch?v=or_Mahv14uQ&t=2081s&fbclid=IwAR1o_SUBsXSJZ4WYXIn4bsKsstqxI95b-CgZRMbnKAanzeOvUyP2xuUbja0

Regeringen, 2018. *National strategi for cyber- og informationssikkerhed - 2018-2021*. Hentet den 4. marts fra: https://digst.dk/media/16815/national_strategi_for_cyber-_og_informationssikkerhed_pdfa.pdf

Rienecker, L. & Stray Jørgensen, P, 2013. *The good paper*. 1. edition: Samfundslitteratur

Sudan, S., 2017. *Det sorte bælte i revision*. FSR Studerende magasinet, s. 5-8. Udgivet august 2017. Hentet den 11. februar fra https://www.fsr.dk/Files/Images/FSR%20Studerende/Magasiner/FSR%20Studerende%20magasin%202017.pdf?fbclid=IwAR0o_g33fZZczC5CykgcH8R6dnqdad5eypnqRm4dC45aKes5A0xfxp45k-U

Rasmus Madsen Carlslund
Cand.merc.aud.
Den 31. maj 2020

Bilag 1: Transskription af spørgsmål og svar ved webinar

Webinar: *Cyber Security-udfordringer i krisetider.* Webinaret er produceret af PwC og de deltagende værter er:

- Natasha Lembke: Partner og Head of Finance Transformation i PwC
- Mads Nørgaard Madsen: Partner og Head of Security and Technology i PwC

https://www.youtube.com/watch?v=or_Mahv14uQ&t=2081s&fbclid=IwAR1o_SUBsXSJZ4WYXIn4bsKsstqxl95b-CgZRMbnKAanzeOvUyP2xuUbja0

34:40-42.05:

Natasha Lembke: Jeg kan se, vi har fået et spørgsmål om, hvordan hele corona-krisen påvirker tilliden til interne kontroller. Det vil komme an på, om man har manuelle interne kontroller, som er meget manuelt funderet, så vil tilliden til det helt sikkert falde. Men hvis man har automatiske og mere indbyggede kontroller i systemerne, så har vi ikke jf. de dialoger jeg har haft, så har vi ikke en forventning om, at det bliver ændret. Så tilliden omkring dem er stadigvæk den samme, men de manuelle er virkelig udsat for det her. Der begynder vi også at sende information på tværs. Det kan være nogle, hvor de ikke lige kan få deres egen mail til at virke, fordi VPN'en ikke har fået adgang. Så har vi set i nogle tilfælde, at så sender de via en privat mail, hotmail eller gmail eller hvad man nu ellers har. Og det er jo forretningskritisk information, man nogle gange sender den vej. Det er rigtig svært. Den anden ting, som vi også har set i trusselsbilledet, det er falske fakturaer. Fordi vi er i en anden setting, end vi normalt er, og nogle af tingene måske applikationer ikke virker, som de plejer, så er der rigtig meget, hvor det bliver sendt forbi en økonomidirektør eller andre steder i forretningen, hvor de lige skal godkende denne her faktura. Så derfor hold fast i de kontroller, I allerede har. Vær virkelig hård på, at de skal gennemføres. Og så selvfølgelig sørge for, at man ikke snyder den ene eller anden vej.

Mads Nørgaard Madsen: Ja, det er den som vi i sikkerhedstermer vil kalde CEO fraud, som ofte har været en landeplage gennem de sidste mange år. Du rammer et meget ømt punkt her: Når alle mennesker pludselig ikke sidder sammen, så bliver vi endnu mere sårbare. Jeg synes også, det er et rigtig godt spørgsmål ift. interne kontroller, for den vil jo blive minimeret. I forvejen var den måske ikke høj nok mange steder, og nu bliver den endnu mere udsat, fordi den ryger ud. Så derfor har vi hele digitaliserings-agendaen, som siger, hvad er det så for nogle ting, vi kan gå ud og gøre, som vi kan få hjælp til og automatisk gøre? Det er der vi gerne på sikkerhedssiden vil sige: For eksempel har vi sådan en servicefunktion vi kalder Manage Cyber Defence og få den rullet ud hos dine agenter og den projekterer, når der sker de her ulovligheder. Jo mere af det her, hvor vi kan bruge den digitale verden eller i hvert fald hjælpe til det. Men vi er der bare ikke i dag, og derfor er der et ekstra risikoområde på det her.

Natasha Lembke: Man kan godt blive meget skræmt, også når man hører i nyheder at andre virksomheder er blevet ramt af det her. Men det nytter ikke noget bare at stikke hovedet ned i jorden og så kigge den anden vej. Tit handler det om at få skabt et overblik: “Hvor står vi overhovedet i dag? Føler vi, at vi er godt med og har vi sat nogle initiativer i gang til at understøtte det her? Eller er vi nødt til virkelig at steppe op ift. at investere og have det her på agendaen?” Og så tror jeg også, at det ville klæde rigtig mange, at det bliver som en del af den ledelsesrapportering, som man har. Så man også kan se: “Hvordan forholder vi os til det fulde risikobillede for vores virksomhed. Ikke kun ift. om vi har konkurrenter eller andre, der kan indtage de markeder, vi har, men hvad er det for en situation, vi står i?”.

Mads Nørgaard Madsen: Det allernemmeste for sikkerheden, det er jo, at man fik en bankocheck fra finance, så slap vi for alt det her (joke)

Griner

Mads Nørgaard Madsen. Og så kunne vi virkelig lave det, der skulle det (joke)

Natasha Lembke: Det kommer ikke til at ske.

Griner

Mads Nørgaard Madsen: Nej, det fornemmer jeg også. Nej, men spøg til side. Jeg tror, at hele det her billede vi ser og udviklingen vi ser i øjeblikket, det pres der er kommet med Covid-19, det sætter et enormt pres på hele digitaliseringsagendaen. Så jeg tror, at mange virksomheder i forvejen har vist, at de skulle den vej. Men nu om de kan lide det eller ej, så er de blevet presset ud i og det skal gøres i et meget højt tempo. Så der ligger jo også nogle muligheder i at være dem, der så tager den her stafet. En af de ting, jeg har set igennem årene, det er, at sikkerhed bliver "brand defining": "Vi er faktisk stolte af, at når du handler med os, så varetager vi dine ting og din informationer og data på en måde, hvor du kan være tryg her". "Det er derfor jeg hellere vil købe denne her service her, end jeg vil købe den der". Så der er et eller andet element i det her, som har en meget strategisk vinkel på det.

Natasha Lembke: Og det er jo både hvis man tager helt ud på forbrugers synspunkt, de er altså meget opmærksomme og følsomme. For hvis du ligesom tager mine bankoplysninger og hvis de bliver frit tilgængeligt for alle andre, så kan banken måske fange noget af det, men ikke i alle tilfælde. Og det samme hvis der bliver lavet identitetstyveri. Så som forbruger kan vi se, at de er enormt følsomme omkring det, men særligt når du også har hele B2B-elementet og handler med andre virksomheder. Tillid er jo simpelthen altafgørende, når vi handler og arbejder sammen. Derfor skal jeg også have tillid til, at din sikkerhed (red. en anden virksomhed) ligeså vel som at min sikkerhed også skal være i orden.

Mads Nørgaard Madsen: Hvis det her skal komme op og køre. Der er ingen tvivl om, at det vi også oplever det er, at de virksomheder, som har haft en hændelse, der

kommer alt der her i fokus med det samme. Jeg plejer at diskutere før, under og efter sagen, men når man bliver ramt og man har hændelsen, sætter det wake-up-call gang i alle actions med det samme. Heldigvis er der jo stadig mange virksomheder, der ikke er blevet ramt, og lad os se om vi kan få det forebygget. Sådan et stykke arbejde, som der er blevet lavet her nu, at det er noget man kan forvente, når de har hørt det her lille indlæg, så kan sikkerhedsafdelingen gå over og banke på døren til finanskontoret og så vil de sammen kunne sætte sig ned og prøve at finde ud af det . Den ene eller anden kan ikke lave det alene.

Natasha Lembke: Og det er måske der, det nogle gange er lidt svært, fordi de ikke naturligt har arbejdet meget sammen, altså de to fagenheder. Men man skal gøre det sammen. De har noget faglig indsigt i og viden om, hvordan trusselsbilledet ser ud, hvad det er der skal til, hvilke effekter det er, vi vil have, når vi sætter forskellige initiativer i gang med at beskytte vores sikkerhed og firewall og andre ting. Vi har til gengæld beregningsmotoren. Vi har en budgetmodel og vi kan sidde og regne på, hvad betyder det så. Sådan så de også kan få lavet de rigtige investeringer, så vi starter det rigtige sted. I stedet for at prøve at løse hele verden på een gang. Man kan ikke undgå det, man kan ikke eliminere risikoen fuldstændig, men hvad er det vi kan gøre for at minimere risikoen. Det har også en effekt, når man ser virksomhedernes rating, så har det faktisk også en effekt. Det kan også have en effekt ift. ens forsikringer, så man forsikringsmæssigt kan få en lavere præmie, hvis man kan bevise og dokumentere på samme måde som sine kontroller, at man egentlig har sat sig ind i det og har styr på det. Men det er en spændende opgave.

Mads Nørgaard Madsen: Det er superspændende og man kan sige, hvis man skal have en opfordring med herfra, så er det i hvert fald at prøve at tage den her dialog ude i virksomhederne.