Bachelorprojekt

6. semester - forår 2021

Eksamensgruppenr.

Gruppenummer: S2125625288

Projekttitel:

Omstillingen til hjemmekontorer i et IT-sikkerhedsperspektiv

Gruppens medlemmer:

Anders Heide Nielsen	66825	aheide@ruc.dk
Jesper Blom Petersen	66495	jblomp@ruc.dk
Magnus Stilling	66423	magnust@ruc.dk
Simon Frederik Støvring	66424	sifrst@ruc.dk

Vejleder:

Henning Christiansen henning@ruc.dk

Dato:

Onsdag, den 9. juni 2021

Abstract

In this paper, we examine what kind of availability and IT-security challenges have occurred during the transition to home workspaces, with a focus on the utilization of VPN-technology.

In order to research this, we performed interviews with remote-working employees and IT-security personnel of large-sized companies, in combination with a thorough technical analysis of the VPN-technology. The intent is to determine how the interplay between managing availability and IT-security have affected the home workspace environments, from both an employee-oriented and technological viewpoint.

The results of our investigations show that the utilization of VPN-technology allowing employees secure access to company resources from home workspaces introduced availability challenges, such as slow connections from data bottlenecks due to an increase in active connections. Additionally, the large-scale transition to home workspaces introduced weak points in the connectivity chain which could cause availability issues, such as loss of internet and system failures, which cut the connection to company resources.

Table of Contents

Indledning

Efter et år med COVID-19 og med påbud om nedlukninger i mange af verdens nationer er der sket store ændringer på arbejdsmarkedet. Dette betyder blandt andet, at flere danskere end nogensinde før er begyndt at arbejde hjemmefra. Dansk Industri har foretaget en analyse af den danske hjemmearbejdssituation, og i denne konkluderes det, at der er sket en stigning på 557% i antallet af hjemmearbejdende siden indtrædelsen af COVD-19. Helt konkret er der sket en stigning fra 70.000 hjemmearbejdende i starten af 2020 til 460.000 hjemmearbejdende per ultimo november 2020. Dansk Industris analyse fremlægger desuden også, at der potentielt set, når de danske COVID-19-restriktioner ophører, vil være en stigning i hjemmearbejdspladser på 128%, i forhold til før COVID-19, eller omtrent 160.000 danskere, der fortsat ønsker at kunne arbejde hjemmefra, hvis det var op til dem selv (Sørensen & Kaldahl, 2021).

Påbuddene om nedlukninger har gjort, at virksomheder har stået overfor et ultimatum om, enten at lukke deres virksomhed eller at finde en måde, hvorpå de kan drive forretningen via fjernarbejde (SMVdanmark, u.d). Når virksomheder omlægger deres interne struktur, fordi det påbydes, at lokationen, hvorfra deres ansatte arbejder, fysisk skal ændres, vil det nødvendigvis være forbundet med udfordringer. Disse udfordringer kan eksempelvis være af personlig, teknisk eller sikkerhedsmæssig art. På det personlige plan kan udfordringerne for eksempel opstå, hvis der ændres på rutiner, eller hvis det nye hjemmearbejdsmiljø, der måske indbefatter tilstedeværelsen af børn, ægtefæller eller andre familiemedlemmer, ikke respekterer, at der udføres arbejde og dermed ikke udøver den nødvendige ro (Kehlet, 2020). Herudover er der tillige de tekniske udfordringer; disse kan eksempelvis forekomme i den hardware, der er blevet udstedt af virksomheden. Måske fungerer en computer ikke efter hensigten, og der er derfor ikke adgang til virksomhedskritiske applikationer og services. Hertil kommer IT-sikkerhedsudfordringerne. Disse udfordringer kan have store konsekvenser for virksomhederne, dersom der ikke tages de nødvendige forbehold. Disse IT-sikkerhedsmæssige udfordringer, der kan findes i omstillingen fra arbejdsplads til hjemmekontor, bliver et centralt omdrejningspunkt for denne rapport.

Især for de mindste danske virksomheder gælder det, at IT-sikkerheden ikke er 'up to code'. Dette kan ses i den screening, Monitor Deloitte foretog på vegne af erhvervsstyrelsen i 2018, hvori mere

end 1000 danske, små og mellemstore virksomheder (SMV'er) indgik. Screeningen viste, at 39% procent af disse virksomheder havde et ikke-tilstrækkelig IT-sikkerhedsniveau, og at 14% af dem havde været udsat for deciderede cyberangreb (Monitor Deloitte, 2018). For de mindste virksomheder, typisk dem uden egen IT-afdeling, gælder det som oftest, at der ikke er ressourcer nok til at styrke virksomhedernes IT-sikkerhed, fordi de ansatte ikke har hverken evner eller tid til at gøre noget ved sikkerhedsproblemerne. På trods af manglende kendskab til IT-sikkerhed i de mindste danske virksomheder kan man godt forstå nødvendigheden af at investere i dette. I de større virksomheder kan der peges på både manglende engagement og manglende forståelse fra ledelsen som årsag til lav investering i IT-sikkerhed (Monitor Deloitte, 2018).

Med en fremtid, hvor der er udsigt til flere fleksible arbejdspladser, altså muligheden for selv at bestemme, hvorfra der arbejdes, skal der nødvendigvis tages højde for at sikre hjemmearbejdspladserne lige så godt som de arbejdspladser, der forefindes i virksomheden. Hjemmearbejde er imidlertid ikke et nyt begreb, men det er nyt, at antallet af hjemmearbejdende er så stort, og dette kan medføre komplikationer, når der skal implementeres nye sikkerhedstiltag i en virksomheds allerede eksisterende datainfrastruktur, eller når sikkerhed og datainfrastrukturer skal nydefineres ude i virksomhederne.

COVID-19-situationen har medført en stigning i nogle specifikke cyberangrebstyper. Især for phishing-angreb er der set en særlig stor stigning. Den amerikanske IT-sikkerhedsvirksomhed, F5, har i deres publikation "2020 Phishing And Fraud Report" skrevet, at der, alene for phishing-angrebstypen, er sket en stigning på 220% i forhold til året 2019, hvor deres tidligere prognosticering foreskrev, at der kun ville ses en stigning på 15% for året 2020 (F5, 2020). Herudover har Microsoft Security foretaget en undersøgelse, der forsøger at afsøge cyberangrebs-landskabet i henholdsvis USA, Storbritannien, Indien og Tyskland. Undersøgelsen er baseret på omkring 800 erhvervsledere og mere end 500 virksomhedsansatte fra virksomheder i de førnævnte nationer. I denne artikel fremlægger erhvervslederne, at phishing-angrebstypen har været den største trussel mod sikkerheden, og at phishing har påvirket hele 90% af de involverede virksomheder, samt at 28% af virksomhederne beklageligvis havde oplevet, at hackere med succes havde angrebet netop deres virksomhed (Microsoft, 2020).

Dansk virksomhedskultur baserer sig i stor grad på tillid. Der kan altså tales om, at der, både hos ledelsen og hos de ansatte, findes tillid til, at IT-sikkerheden alene kan varetages af virksomhedens IT-sikkerhedskyndige. Problemet er dog imidlertid, at IT-sikkerhed er et virksomhedsomspændende fænomen, alle skal tage del i, før det kan betegnes som værende effektivt (ASCD, 2020). I en rapport udarbejdet af forskere fra Syddansk Universitet og IT-Universitetet afdækkes det, at ansatte i danske SMV'er mangler træning og undervisning i IT-sikkerhed, og dette endda på trods af, at virksomhedsledere faktisk er parate til at investere i IT-sikkerhedsundervisning. Problemet er bare, at træningen og undervisningen som regel først bliver sat i værk, hvis der kommer forespørgsler fra de ansatte selv (ASCD, 2020, 46). Dét, at ansvaret for, at der bliver undervist i IT-sikkerhed, ligger hos den enkelte medarbejder, kan betyde, at det nedprioriteres til fordel for enten andre arbejdsopgaver eller undervisning, der relaterer sig direkte til vedkommendes egentlige arbejde (ASCD, 2020).

Under COVID-19 og de påtvungne hjemmearbejdspladser har hver enkelt ansat, i højere grad end normalt, måtte fungere som sin egen IT-medarbejder, dersom der skulle opstå tekniske problemer i forbindelse med deres arbejde. Dette kan være en stressfaktor for de ansatte, der ikke er teknisk kyndige, og det kan være et problem rent sikkerhedsmæssigt, at den enkelte medarbejder ikke har den nødvendige viden om, hvordan et sikkerhedsbrud skal håndteres (Arildsen, 2020). I en undersøgelse fra 2019 foretaget af virksomheden Kaspersky, baseret på 4958 informanter spredt over 23 forskellige lande i henholdsvis Nord- og Sydamerika, Europa og Asien, kan det udledes, at sikkerhedsbrud forårsaget af ansatte kan resultere i personlige konsekvenser for vedkommende. Disse konsekvenser kan eksempelvis blive økonomiske, familierelaterede eller tidsmæssige. Kasperskys undersøgelse fremlægger, at 15% af ansatte, der har været årsag til et sikkerhedsbrud, bliver frataget eventuelle monetære bonusser. Fra samme undersøgelse kan det ses, at 32% bliver pålagt overarbejde, 27% må give afkald på pauser, weekender og ferier, 33% føler et højere stressniveau end normalt, og at 16% af tilfældene oplever at modtage en disciplinærstraf (Kaspersky, 2019, 8).

Hjemmekontorer er imidlertid ikke et nyt fænomen. De har været en del af de fleste større virksomheders fleksible tilgang til at få arbejde gennemført og til at opretholde produktivitet under forhold, hvor tilstedeværelsen på virksomhedskontoret af forskellige årsager ikke er mulig, dog ikke i så bemærkelsesværdig en størrelsesorden som i COVID-19-situationen.
En af de primære teknologier, der baner vejen for effektivitet af hjemmekontorer, er VPN-teknologien (Virtual Private Network). Denne kan bidrage til både IT-sikkerhed og integriteten af virksomhedens data, når disse behandles på hjemmekontorerne, samt i højere grad at tillade ansatte at tilgå virksomhedens ressourcer, uden at de fysisk befinder sig på virksomhedens arealer. Idet denne teknologi er et af de vigtigste knudepunkter, der tillader den storstilede omstilling til hjemmearbejde, mener vi, at undersøgelsen af denne teknologi, og effekterne af dens benyttelse i sammenhæng med de ændrede arbejdsforhold, er af stor relevans, hvad angår at undersøge og analysere udfordringer ved omstillingen til hjemmekontorer.

Med ovenstående in mente er der forhåbentlig skabt et billede af, at der er mange steder, der kan sættes ind i forhold til IT-sikkerhed. Vi har valgt at undersøge, hvilke udfordringer, der har kunnet findes ved omstillingen til hjemmekontorer, og hvordan VPN-teknologien har haft indflydelse herpå.

Grundlaget for dette projekt skal findes i en fælles interesse iblandt projektdeltagerne for emnet IT-sikkerhed. IT-sikkerhed har været et gennemgående tema i projektgruppens 3 forrige projekter, og det var derfor naturligt at fortsætte ud af denne IT-sikkerhedsmæssige tangent. Vi finder IT-sikkerhed særligt interessant, fordi det er et meget omfattende felt, der er i konstant udvikling. Der er altså hele tiden noget nyt at undersøge og fordybe sig i. Herudover er kampen mellem hacker og IT-sikkerhedsprofessionelle en evig kilde til beundring, da de IT-sikkerhedskyndige altid skal være to skridt foran i forhold til nye angrebsstrategier og nye angrebsmetoder. Den store efterspørgsel på IT-sikkerhedsprofessionelle er også en klar drivfaktor, da det vil blive muligt at komme ud og gøre en reel og eftertragtet forskel i en virksomhed, dersom der tages yderligere uddannelse indenfor feltet og søges arbejde her.

Med projektet ønsker vi at undersøge og afdække såvel udfordringerne, der har været i forbindelse med omlægningen til hjemmekontorer, som VPN-teknologien og dens iboende drivkræfter og barrierer. Vi har tidligere arbejdet med ISO27000-standarden og har fået en generel forståelse for, hvordan IT-sikkerhed skal administreres. Hertil vil vi nu udbygge vores viden omkring IT-sikkerhed ved at undersøge de specifikke komplikationer, der har været i forbindelse med COVID-19, og ved på nært hold at undersøge VPN-teknologien som sikkerhedsmekanisme.

Empiriindsamlingen for projektet kommer til at bestå af semistrukturerede interviews af henholdsvis IT-sikkerhedsprofessionelle og hjemmearbejdende ansatte. Interviewene med de IT-sikkerhedsprofessionelle skal hjælpe til at få en forståelse for, hvad der var planlagt for omstillingen, og interviewene med de hjemmearbejdende skal give et indblik i, hvad der er sket rent praktisk. Ydermere stiller vi os på skuldrene af andre publikationer, der omhandler IT-sikkerhed generelt og IT-sikkerhed under COVID-19-pandemien.

Problemformulering

"Hvilke udfordringer har der været med data-tilgængelighed i forbindelse med hjemmekontorsomstillingen, og hvilken indflydelse har VPN-teknologien haft herpå?"

Arbejdsspørgsmål

- Hvordan undersøger vi VPN som teknologi?
- Hvilke problemstillinger findes der ved omstilling til hjemmekontorer?
- Hvilke krav findes der fra virksomheder ift. hjemmekontorer og sikkerhed?
- Hvordan efterlever ansatte deres virksomheds retningslinjer for it-sikkerhed på hjemmekontorerne?
- Hvilke tanker gør ansatte sig om sikkerheden på deres hjemmekontor?

De humanistisk-teknologiske dimensioner

Dette projekt er skrevet inden for det Humanistisk-Teknologiske fagområde. Dette betyder, at projektet inddrager de tre konstituerede dimensioner, den Humanistisk-Teknologiske bachelor-uddannelse forankres i. Det drejer sig om dimensionerne: Design og Konstruktion (D&K), Subjektivitet, Teknologi og Samfund (STS) og Teknologiske Systemer og Artefakter (TSA). Formålet med denne inddragelse af dimensionerne er at skabe en nuanceret tilgang til projektets problem-stilling. Vi har tænkt os at benytte metoder og teori fra de forskellige dimensioner som grundlag for og underbygning af arbejdet med projektet.

Dimensionen Design og Konstruktion er forankret i en designvidenskabelig tradition og har fokus på udvikling og evaluering af systemer, processer og artefakter. Der trækkes i dimensionen på teorier og begreber om design og konstruktion. Metoderne og værktøjerne i dimensionen fokuserer på at understøtte og organisere designprocesser. Formålet med dimension er at skabe baggrundsviden og færdigheder til at skabe processer og/eller produkter, der tjener menneskelige formål (Pries-Heje, 2018, 1-2).

Dimensionen Subjektivitet, Teknologi og Samfund handler om mennesker og den teknologi, de skaber og interagerer med. Dimensionen giver historisk, social, kulturel og miljømæssig viden omkring teknologi. Yderligere bearbejdes etnografiske problemstillinger, hvilket giver værktøjer til empiriindsamling. Det handler om at udforske handlemuligheder og rum for demokratisk deltagelse i vore dages teknologimedierede samfund (Sommer, 2018, 2).

Dimensionen Teknologiske Systemer og Artefakter leverer et værktøj, der kan anvendes til at analysere og forstå en teknologi. Et grundlæggende værktøj i dimensionen er TRIN-modellen, som er en ny måde at beskrive og tilgå en teknologi på.

Projektets problemformulering passer ind i paradigmet Subjektivitet, Teknologi og Samfund og i paradigmet Teknologiske Systemer og Artefakter. Begrundelsen for dette er, at den første del af problemformuleringen, *Hvilke udfordringer har der været med data-tilgængelighed i forbindelse med hjemmekontorsomstillingen*, handler om, hvordan teknologi kan have indflydelse på

mennesker, og særligt deres arbejdsliv. Denne del knytter sig til dimensionen Subjektivitet, Teknologi og Samfund. Den anden del af problemformuleringen, *hvilken indflydelse har VPN-teknologien haft*, handler om at forstå en specifik teknologi, fordi denne har haft stor indflydelse på problemstillingen og knytter sig til dimensionen Teknologiske Systemer og Artefakter.

Når det kommer til, hvordan de tre dimensioner specifikt er inddraget i projektet, kan det nævnes, at projektets indsamling af primær-empiri er sket gennem semistrukturerede interviews, som hører under dimensionen Subjektivitet, Teknologi og Samfund. Ydermere bruges STS-dimensionen i projektet til at forsøge at forklare nogle af de samfundsmæssige problematikker, empirien belyser.

I projektet benyttes TRIN-modellen fra dimensionen Teknologiske Systemer og Artefakter til at kortlægge og undersøge VPN-teknologien. TRIN-modellen er et værktøj til at beskrive og forstå en teknologi, og som tillige afsøger at give en fyldestgørende dækning af teknologien og eventuelle skjulte aspekter ved den.

Design og Konstruktions-dimensionen inddrages særligt i projektets perspektivering. Denne perspektivering handler om tidligere projekter, hvor der er arbejdet i med IT-sikkerhed i mikro-virksomheder. Her vil vi diskutere, hvordan en designløsning, omhandlende resultaterne fra dette projekt, vil kunne afhjælpe nogle af de problemstillinger, mikro-virksomheder har i forhold til IT-sikkerhed.

Teorier og metoder

Videnskabsteori

Ved videnskabsteori undersøges der, hvilke metoder, der skaber viden, ud fra en filosofi om, hvad der er sandhed, og hvilke kriterier, der kendetegner dette. Det er en teori om årsagssammenhænge, der skal give en forståelse for ny viden inden for et felt og undersøge, om den viden, der bliver skabt, kan sættes i perspektiv til et større verdensbillede (Vestergård, 2010). Teorien om at skabe viden tog sin form på et metaplan ved filosofien om logisk positivisme, hvor forudsætningen for sandhed byggede på, induktivt at verificere en sandhedspåstand ved at efterprøve denne. Senere kom filosofien om falsifikation, som omhandlede at formulere en teori med hypoteser, hvorefter denne søges modbevist indtil teorien accepteres som sandfærdig (Sismondo, 2010, 2-4). Siden da er der udviklet flere videnskabsteorier med forskellige filosofier, men siden det, der kaldes "the Kuhnian Revolution" (red. Thomas Kuhn), har fællesnævneren for videnskabsteorier været undersøgelsen af paradigmer, altså den forståelseshorisont, der kendetegner et felt. Et paradigme skal forstås som den viden, der er skabt inden for et felt, hvor forskere i feltet har en fælles anerkendelse af eksisterende viden herom, samt konsensus om, hvilke metoder og teorier det er korrekt at anvende for at danne ny viden indenfor det givne felt (Sismondo, 2010, 11).

Casestudier

Ved definitionen af et casestudie beskrives et studie eller en observation af et fænomen, der har til formål at bekræfte og danne kontekst til en teori, eller helt at afkræfte en given teori. Dette betyder dog ikke, at enkelte casestudier skal producere teoretisk repræsentative resultater for at klassificeres som succesfulde, men kan i stedet bidrage til viden om sub-aspekter i teorien, eller skabe nye aspekter af viden til feltet (Madsen, 2009 ¶ case-studie).

I forhold til et videnskabsteoretisk blik på casestudiet, produceres der en kontekstuel viden, som Flyvbjerg beskriver som dét, der udvikler vidensfeltet til et dybere plan, og derved skaber en ekspertlig forståelse af feltet. Argumentet om casestudiers videnskabsteoretiske sammenhænge ses derfor ved muligheden for at udtænke og afprøve hypoteser, der kan medføre et vidensbidrag til et fænomen uden at følge en regelfast generalisering. (Flyvbjerg, 2006, 221-229).

I nedenstående tabel beskriver Flyvbjerg måder, hvorpå et casestudie kan gribes an, samt hvordan disse casetyper bidrager til ny viden.

Table 1
Strategies for the Selection of Samples and Cases

Type of Selection	Purpose
A. Random selection	To avoid systematic biases in the sample. The sample's size is decisive for generalization.
1. Random sample	To achieve a representative sample that allows for generalization for the entire population.
2. Stratified sample	To generalize for specially selected subgroups within the population.
B. Information-oriented selection	To maximize the utility of information from small samples and single cases. Cases are selected on the basis of expectations about their information content.
1. Extreme/deviant cases	To obtain information on unusual cases, which can be especially problematic or especially good in a more closely defined sense.
2. Maximum variation cases	To obtain information about the significance of various circumstances for case process and outcome (e.g., three to four cases that are very different on one dimension: size, form of organization, location, budget).
3. Critical cases	To achieve information that permits logical deductions of the type, "If this is (not) valid for this case, then it applies to all (no) cases."
4. Paradigmatic cases	To develop a metaphor or establish a school for the domain that the case concerns.

Figur 1. Flyvbjerg, 2006, 230

Som tabellen viser, kan casestudiet skabe forskellige vidensresultater, alt efter hvilken strategi, der anvendes. Den ene type casestrategi søger enten at eliminere bias eller at klassificere cases ved at tage udgangspunkt i tilfældigt udvalgte cases, hvor den anden type casestrategi har et informationsorienteret udgangspunkt (Flyvbjerg, 2006, 229-230).
Ud fra disse overvejelser har vi planlagt en paradigmatisk casestrategi, eftersom den viden, vi søger at få ud af undersøgelsen, skal have til formål at kortlægge virksomheders retningslinjer, hvad angår IT-sikkerhed og beskyttelse af data ved ansattes omstilling til hjemmekontor. Den viden, vi får ud af vores empiriarbejde, skal derved samle en anskuelse af feltet og skal potentielt kunne bidrage til IT-sikkerhedsrelateret teori, såsom Confidentiality, Integrity & Availability (CIA), og risikoanalyse, samt problemstillinger ved omstilling til hjemmekontorer.
Fremadrettet vil de cases, der er udvalgt i denne rapport, omtales som interviews med informanter, der enten er hjemmearbejdende eller IT-sikkerhedspersonale/ansvarlige.

Hvad er IT-sikkerhed?

Dette afsnit har til formål at redegøre for, hvordan IT-sikkerhed defineres, hvad IT-sikkerhed indebærer, og hvorfor IT-sikkerhed er relevant. Afsnittet indledes med en universel IT-sikkerhedsudfordring, denne følges op af en introduktion til sikkerhedstriaden og slutteligt følger redegørelser for forskellige trusselstyper, sårbarhed, sandsynlighed, impact og risiko.

Selvom både den globale digitalisering og frekvensen af cyberangreb er stigende, er IT-sikkerhed i mange tilfælde stadig et fænomen, der implementeres som blot en eftertanke (Stallings & Brown, 2018, 29). Hvis ikke sikkerhed implementeres allerede i designfasen, når der udvikles nye IT-systemer, kan det i sidste ende forårsage ikke-tilsigtede sårbarheder i disse systemer. I disse tilfælde bliver brugerne af IT-systemerne nødt til at købe sig til, eller selv at udvikle, egne sikkerhedsforanstaltninger, der kan kobles udenpå IT-systemet for at gøre det sikkert (Ingham, 2020, u.s.). En bedre IT-systemudviklingspraksis skal findes i at prioritere IT-sikkerhed allerede i designfasen og sikre, at denne sikkerhedsprioritering holder ved hele vejen igennem IT-systemets udviklingsfase (Stallings & Brown, 2018, 29). Det forholder sig sådan, at fænomenet IT-sikkerhed kun eksisterer, fordi der findes en kontinuerlig kamp mellem IT-kriminelle og IT-sikkerhedsprofessionelle. Den kriminelle forsøger at finde sårbarheder i et IT-system, og de sikkerhedsprofessionelle forsøger at eliminere disse sårbarheder. Den kriminelle har en evig fordel, fordi vedkommende blot skal finde én enkelt sårbarhed, der kan udnyttes. For IT-sikkerhedspersonalet gælder det om at være opmærksom på alle de iboende sårbarheder, der findes i de IT-systemer, de varetager (Stallings & Brown, 2018, 29). Er der herfor tale om IT-systemer, hvor der fra start ikke er indtænkt sikkerhed, og hvor sikkerhedstiltag altså først er tilføjet som efterfølgende 'lappeløsninger', kan det vise sig mere besværligt end ellers at holde kriminelle på afstand.

Ord såsom sårbarhed og sikkerhed er selvfølgelig nogle let brugte termer, der dækker over for mange ting på én gang til, at deres egentlige betydninger fremstår tydelige. Af denne grund vil vi i

det efterfølgende konkretisere, hvordan IT-sikkerhed hænger sammen på en mere metodisk og struktureret måde.

NIST, National Institute of Standard and Technology, definerer IT-sikkerhed således:

> *"Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored and communicated."*
>
> (Stallings & Brown, 2018, 24)

På baggrund af denne definition, og med især information eller data in mente, må det ultimative mål med IT-sikkerhed altså være at tilgængeliggøre information for autoriserede personer, sørge for at integriteten af denne information ikke svækkes, samt at hemmeligholde samme information for ikke-autoriserede personer (Pfleeger, Pfleeger, Margulies, 2015, 7). Sikkerhedstriaden (the CIA triad) er en model, der beskriver netop dette mål. Sikkerhedstriaden udgøres af principperne om fortrolighed (confidentiality), integritet (integrity) samt tilgængelighed (availability), og disse principper udgør tilsammen en ramme for, hvordan informationssikkerhed kan gennemtænkes og håndteres (Stallings & Brown, 2018, 29).

Fortrolighed

Princippet om fortrolighed sikrer på et overordnet plan, at information kun kan ses eller tilegnes af autoriserede personer eller systemer. Fortrolighedsprincippet er altså det, der skal sikre, at uvedkommende ikke kan se eller opspore information, data eller udstyr, de ikke burde have adgang til (Pfleeger, et al., 2015, 7). Fortrolighedsprincippet handler i høj grad om at afskærme data eller information og om adgangskontrol. Selve adgangskontrollen kan forstås, som om der gives enten et ja eller et nej til enten en person eller et system, der prøver til at tilgå noget information på en forudbestemt måde. Det vil sige, at en person kan være autoriseret til at tilgå et stykke data på én måde, men måske ikke være autoriseret til at tilgå samme data bare på en anden måde (Pfleeger, et al., 2015, 9). Med hensyn til data-afskærmning kan der eksempelvis være tale om et fortrolighedsbrud, hvis en person på uautoriseret vis får adgang til noget data, eller hvis denne

person tilegner sig viden om eksistensen af noget information, der burde have været hemmeligholdt. Selv det, blot at vide at noget data eksisterer, uden at vide, hvad det konkret består af, er nemlig også et brud på fortroligheden (Pfleeger, et al., 2015, 9).

Integritet

Princippet om integritet sikrer, at data eller information er brugbart og ikke kan modificeres uden at subjektet, der modificerer det, er autoriseret hertil. Integritet sikrer altså, at kun en person eller et system med læse- og skriverettigheder til et bestemt stykke data, kan få lov til at modificere det (Pfleeger, et al., 2015, 10). Der kan også tales om integritet i forbindelse med måden, hvorpå data eller information bliver modificeret. Det er nemlig ikke sikkert, at alle måder, at modificere data eller information på, er acceptable, hvorfor disse måske ikke er en lovlig måde at ændre data på (Pfleeger, et al., 2015, 11). Ligesom med princippet om fortrolighed kan informations- og dataintegritet kontrolleres med adgangskontroller. Det skal altså forudbestemmes, hvem eller hvad, der kan modificere information, og på hvilke måder, det må modificeres. Herudover kan logging af præcis hvem eller hvad, der tilgår data, og hvordan denne data bliver modificeret, også været et godt værktøj til at identificere integritetsbrud (Pfleeger, et al., 2015, 11).

Tilgængelighed

Princippet om tilgængelighed sikrer, at data og information er intakt, og at det kan fremfindes, uanset hvornår det ønskes (Pfleeger, et al., 2015, 11). Der er typisk ofte fokus på hardware i forbindelse med princippet om tilgængelighed. Det er nemlig tit hardware, der får skylden, hvis der ikke kan skabes forbindelse til noget data, eller hvis services ikke kan benyttes (Pfleeger, et al., 2015, 11). I princippet om tilgængelighed ligger også, at kapaciteten af en service er tilstrækkelig til den trafik, der sendes til den, samt det, at servicen skal være udført indenfor et acceptabelt tidsrum (Pfleeger, et al., 2015, 12). Desuden skal disse services være i stand til at afgive fejlmeldinger, ifald der opstår fejl, og skal herudover også være i stand at lave elegante serviceophør, uden at data eller information går tabt i processen (Pfleeger, et al., 2015, 12).

Andre relevante principper

Udover de førnævnte principper, fortrolighed, integritet og tilgængelighed, findes der også et par andre relevante principper, som kan være med til at højne forståelsen af IT-sikkerhedsmålet. Principperne om forklarlighed (accountability) og autenticitet (authenticity) er nogle typiske sikkerhedstriadetilføjelser, især hvis der benyttes kommunikationssystemer. Princippet om forklarlighed sikrer, at handlinger, foretaget af enten personer eller systemer, kan spores, samt at disse personer eller systemer ikke kan afvise at have udført denne handling (Pfleeger, et al., 2015, 7). Princippet om autenticitet sikrer, at personer eller systemer er, hvem de giver sig ud for at være. Det er dette princip, der skaber tillid til, at handlinger, udført af en person eller et system, er udført af netop den person eller det system, og at de står inde for den udførte handling (Pfleeger, et al., 2015, 7).

Herudover findes der også principper om privatliv (privacy) og auditeringsevne (auditability) (Srivathsav, 2020, u.d.). Princippet om privatliv sikrer muligheden for, at der eksempelvis ikke deles sensitive, personlige attributter, som måtte være indlejret i et aktiv eller i et system. Princippet om auditeringsevne sikrer, at alle handlinger, der er rettet mod data eller information, skal kunne auditeres. Ved auditering skal resultaterne fra den interne og den eksterne auditering være ensartede (Srivathsav, 2020, u.d.).

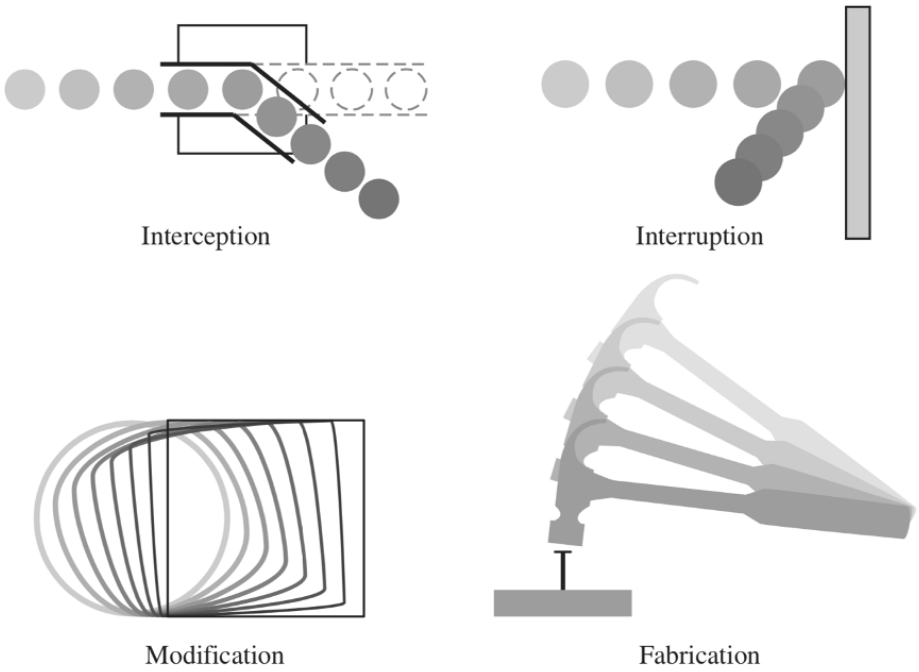
Trusler

Trusler i en IT-sikkerhedsmæssig sammenhæng er et sæt af omstændigheder, der har potentiale til at forårsage tab eller skade. Trusler kan findes i de fleste ting, som kan have indflydelse på funktionen eller informationen i et IT-system. Hardwarefejl, software-crashes og menneskelige fejl er alle ganske normale typer af trusler, der forekommer med hyppig frekvens, men der kan også findes trusler i forbindelse med naturkatastrofer, som i værste fald kan medføre ødelæggelse af udstyr og dermed kan gøre et IT-system ikke-funktionsdygtigt (Pfleeger, et al., 2015, 6).

Trusselstyper

Der findes fire overordnede trusselstyper, som kan føre til brud på IT-sikkerheden. Det er disse trusselstyper, sikkerhedstriaden skal sørge for, ikke forekommer, og trusselstyperne kan derfor ret

præcist pinpointes til en eller flere af principperne fra sikkerhedstriaden. De fire trusselstyper udgøres af aflytning (interception), afbrydelse (interruption), modifikation (modification) og fabrikation (fabrication) (Pfleeger, et al., 2015, 8).



(Figur 2. Pfleeger, et al., 2015, 8).

Aflytning

Aflytningstruslen lægger sig op ad princippet om fortrolighed. Truslen ligger nemlig i, at der potentielt kan være en person eller et system, der opsnapper viden, information eller data, som bliver kommunikeret, overført eller på anden måde behandlet. Konkrete eksempler kan være wiretapping eller at kopiere data uden tilladelse (Pfleeger, et al., 2015, 8).

Afbrydelse

Afbrydelsestruslen er relevant i forbindelse med princippet om tilgængelighed. I truslen ligger det, at eksempelvis en service kan blive stoppet eller at data kan forsvinde. Konkrete eksempler kan være ødelæggelse af hardware eller installation af datadestruerende malware (Pfleeger, et al., 2015, 8).

Modifikation

Modifikationstruslen kan sættes sammen med princippet om integritet. Modifikationstruslen dækker over muligheder for, at personer eller systemer eksempelvis kan ændre software eller hardware, men også at der kan ændres på data, eksempelvis databaser (Pfleeger, et al., 2015, 8).

Fabrikation

Ligesom med modifikationstruslen, falder truslen om fabrikation også ind under princippet om integritet. Fabrikationstruslen dækker over muligheden for, at personer eller systemer kan fabrikere falsk data. Eksempelvis betyder dette, at der potentielt kan oprettes tabeller i en database, eller at der kan tilføjes ikke tilladte udvekslinger mellem enheder på et netværk (Pfleeger, et al., 2015, 8).

Sårbarheder

Sårbarheder er de deciderede svagheder, der kan findes i IT-systemer eller tekniske artefakter. Det er disse sårbarheder, der udnyttes, når der udføres angreb på IT-systemer og IT-udstyr (Pfleeger, et al., 2015, 6). En sårbarhed afviger fra en trussel, fordi det er en konkret svaghed i et givent system eller artefakt, hvor trusler i større grad betegnes som den negative handling, der udføres mod sårbarheden. En eksemplificering kan være en router, hvor default-bruger og -kodeord ikke er ændret. Det, at disse to parametre ikke er ændret, er en sårbarhed, da en vilkårlig person med kendskab til denne type router ville kunne ændre førnævnte parametre og dermed have kontrol over routeren. Så længe personen ikke tager kontrol over routeren, er det en sårbarhed, men så snart personen udfører handlingen, bliver det en trussel.

Sandsynlighed

Sandsynlighed definerer niveauet af, hvorvidt noget kommer til at ske. En typisk tidsramme for sandsynlighedsberegninger omhandlende sikkerhedstrusler er et år. Her beregnes det altså, hvor stor chancen er for, at en specifik trussel, rettet mod en specifik sårbarhed sker i løbet af et år (Pfleeger, et al., 2015, 26). Sandsynlighed kan måles på to måder; kvantitativ og kvalitativ sandsynlighed. Ved kvantitativ sandsynlighed kan der ses på historiske data for frekvensen af, at noget sker. Et eksempel kunne være strømforsyningen i en server. Producenten har nogle

historiske data over fejlraten for strømforsyningerne i deres servere. Disse data kan bruges til at undersøge, hvor stor frekvensen er for, at netop denne strømforsyning bliver ikke-funktions dygtig. Ved kvalitativ sandsynlighed bliver der benyttet kvalitative metoder til at finde et sandsynlighedsniveau. Der bliver typisk målt i skalaer af "lav-mellem-høj" eller andre specielt indrettede skalaer, der kan bistå den sandsynlighed, der skal beregnes. Et eksempel kunne være at finde sandsynligheden for, at en gruppe medarbejdere kunne være årsag til et IT-sikkerhedsbrud. Der ville i denne forbindelse blive foretaget nogle undersøgelser af denne gruppe ansattes digitale adfærd. Dette kan så sættes ind i et grid, hvorudfra en sandsynlighed kan defineres gennem resultaterne fra undersøgelsen af deres digitale adfærd (Bilag 2).

Impact

Impact er den faktiske skade, der forårsages af en trussel. Impact er altså det skadesresultat, der opstår, når en specifik trussel overføres på en specifik sårbarhed. Impact kan ligesom sandsynlighed beskrives på to måder; kvantitativ og kvalitativ (Pfleeger, et al., 2015, 26). Ved en kvantitativ beskrivelse af impact kan der eksempelvis kigges på de omkostninger, der har været i forbindelse med et IT-angreb; der kan måles på, hvor meget arbejde, der går tabt på grund af et IT-angreb, eller der kan måles på den mistede tid, det tager at rette op på følgerne af et IT-angreb. Et eksempel kunne bygge på en ikke-funktionsdygtig server; hvilke omkostninger følger, i forhold til at få serveren repareret? Hvor meget arbejde er gået tabt, eller hvor meget arbejde kan ikke udføres, så længe serveren er ude af drift? Hvor lang tid tager det at få serveren op at køre igen? Ved en kvalitativ beskrivelse af impact kan der ses på eksempelvis omdømme. En eksemplificering kunne være, hvordan en virksomheds omdømme fremstår, efter at deres webserver har været ude af drift, og kunder derfor ikke har kunnet besøge virksomhedens hjemmeside.

Risiko

Risiko er produktet af en trussel og denne trussels iboende hændelsessandsynlighed, der overføres på en sårbarhed, samt den impact, dette medfører.

$$Risiko = Trussel * Sårbarhed * Impact$$

Ovenstående er en generisk formel for, hvordan risiko kan anskues. Den forklarer, hvordan sammenhængen mellem trussel, overført på sårbarhed og dennes impact udgør en risiko. Risiko er en størrelse, der skal defineres, så det giver mening i den sammenhæng, hvori det skal bruges.

Interview

Ved at tage udgangspunkt i det videnskabsteoretiske aspekt om vidensdannelse, ses der en epistemologisk tilgang til dette, ved interview som empiriindsamlingsmetode. Epistemologien søger at skabe viden ud fra sanseindtryk og italesættelse heraf, hvilket vil sige, at interviews bidrager til en epistemologisk videnskabelse.

Indsamlingen af empiri fra projektets informanter foregår gennem semistrukturerede interviews med flere virksomheders ansatte og IT-sikkerhedsansvarlige. Vi har valgt at benytte os den semistrukturerede interviewmetoder med den bevæggrund, at forholdene for de ansatte er forholdsvis nye, og der dermed kan forekomme hidtil ikke-forventede handlinger og motivationer hos de ansatte, som med fordel kan uddybes ved benyttelsen af en mere fleksibel interviewmetode.

Semistrukturerede interviews er en kvalitativ empiriindsamlingsmetode, der tillader en mere fleksibel tilgang til interviewforløbet, ved at sætte det primære fokus på informantens egne oplevelser og udtalelser, og give plads til at stille uddybende spørgsmål på baggrund af netop disse udtalelser (Brinkmann & Tanggaard, 2015, 37-40). Det semistrukturerede interview er en hybrid af det løst strukturerede interview og det stramt strukturerede interview, og det låner elementer fra begge. Denne interviewmetode er derfor mere fleksibel i sin empiriindsamling end den stramt strukturerede metode, når det kommer til subjektive holdninger og udtalelser, men den tillader også intervieweren at indhale en drivende samtale, således der ikke mistes fokus på undersøgelsesområdet (Brinkmann & Tanggaard, 2015, 37-40).

Som understøttelse af denne interviewforms mere fleksible fremgangsform udarbejdes der ofte en tilhørende interviewguide, som intervieweren benytter til at bevare interviewets fokus på det, der undersøges. Interviewguiden er struktureret således, at spørgsmålene agerer som springbræt til en videre samtale om emnet, og dermed ikke som strikse sæt af spørgsmål, som informanten skal besvare (Brinkmann & Tanggaard, 2015, 37-40).

Interviewguide

Vi har valgt at inddrage både IT-sikkerhedsansvarlige og hjemmearbejdende ansatte for at få en bredere forståelse af forholdene i virksomheden, og disse er opdelt i deres egne interviewguider. Interviewguiderne er sammensat således, at intervieweren altid kan holde intentionen bag et spørgsmål for øje ved at kigge på indholdsspalten. Forskellen mellem forskningsspørgsmålet og interviewspørgsmålet ligger i, i hvilken kontekst disse to bruges. Forskningsspørgsmålet er intenderet til internt brug i forskningsgruppen, og interviewspørgsmålet er så det, der præsenteres for interviewets informant. Spørgsmålene i vores interviewguide er farveopdelte; de blå spalter er til intern brug i gruppen, og den grønne spalte er de spørgsmål, vi stiller vores informanter.
De fulde interviewguides til både ansatte og IT-ansvarlige findes i bilagsdokumentet fra side 2 til 13.

De interviews, vi har foretaget, er med informanter, der enten repræsenterer hjemmearbejdende ansatte eller ansatte i virksomheders IT-afdeling. Vi har foretaget interviews med fem informanter, der er hjemmearbejdende ansatte, som hver repræsenterer forskellige virksomheder i forskellige størrelser, dog er majoriteten af informanterne ansat i store virksomheder med mere end 250 ansatte. Derudover har vi interviewet to informanter, som repræsenterer ansatte i en stor virksomheds IT-afdeling, hvor den ene har et teknisk ansvar, og den anden har ansvar for IT-sikkerhedsprotokoller. Alle informanterne og de virksomhederne, de repræsenter, er anonyme, og informationen om virksomhederne er begrænset, men det kan nævnes, at informanterne repræsenterer servicevirksomheder, justitsministeriets ressort og sundhedsministeriets ressort. Servicevirksomhederne leverer forskellige produkttyper, hvorfor deres data og risikoniveauet varierer, hvilket betyder at informanternes udsagn ligeledes kan variere som resultat af dette.

TRIN-modellen

TRIN-modellen er en metode, der overordnet har til formål at beskrive, definere og analysere en teknologi. Metoden består af 6 'trin', som hver især fokuserer på et teknisk-videnskabeligt aspekt omkring en teknologi. Trinnene er som følger:

1. Identifikation og analyse af en teknologis **indre mekanismer og processer**.
2. Identifikation og analyse af teknologiens **artefakter**.
3. Identifikation og analyse af en teknologis **utilsigtede effekter**.
4. Analyse af sammenhænge i større **teknologisystemer**.
5. Opstille en **model** af en teknologi.
6. Analyse af drivkræfter og barrierer for **udbredelse af innovationen**.

Disse 6 trin lægger op til en sammenfatning og perspektivering af den specifikke teknologi, metoden benyttes på (Jørgensen, 2018, s. 2-5)

TRIN-modellen trækker på anerkendte definitioner af teknologi og er baseret på disse. Heriblandt nævnes Carl Mitchams argument for, at enhver teknologi består af de fire elementer:

Objekt – er den fysiske entitet, som teknologien udgør;

viden – bagvedlæggende teori og viden inden for det, som teknologien bliver konstrueret til formål for;

aktivitet – processen i udviklingen af teknologien, samt vedligeholdelse og brug af den;

og *vilje* – formålet og grunden til, at denne teknologi eksisterer.

TRIN-modellen til analyse af teknologier forholder sig kritisk til denne teknologidefinition, eftersom den fokuserer på konstruktionen af fysiske artefakter og tilsidesætter udvikling af

teknologier, som for eksempel kan være nye arbejdsgange, protokoller eller læringsprocesser – altså teknologiudvikling, som ikke er artefakter. Derudover fremstår Mitchams beskrivelse af teknologi ikke som værende analyseorienteret, hvorfor TRIN-modellen trækker på en definition af Müller, der overvejende fokuserer mere på udviklingsprocessen og teknologien som det færdige produkt.

Müllers definition indeholder analyseaspektet, som er savnet i Mitchams definition, dog med et primært fokus på arbejdsprocesser. TRIN-modellen bygger videre på Mitchams teknologidefinition og tilfører yderligere Müllers analyseaspekt gennem tilføjelse af utilsigtede effekter og drivkræfter.

I dette projekt vil vi bruge TRIN-modellen på VPN-teknologien. Formålet, med at bruge denne metode, er at give en bred forståelse af en teknologi, som har været central for omstillingen til hjemmekontorer. Det er meningen, at denne metode skal bruges til at give indblik i vidensområdet omkring hjemmekontorer og specifikt IT-sikkerheden på disse. Ligeledes skal kortlægningen og sammenfatningen af VPN-teknologien gennem denne metode bruges til at perspektivere til andre elementer indenfor vidensområdet.

Vi anvender TRIN-modellen for at analysere den teknologi, vi mener kan bidrage til at undersøge den overordnede problemstilling omkring sårbare virksomhedsdata på hjemmekontorer. Denne teknologianalyse er derfor ikke tænkt som den hovedanalyse, rapporten skal baseres på. Den anvendes som led i at eksplicere, hvad en VPN-forbindelse er, hvilket formål den tilsigter, og hvorfor vi synes, at netop denne teknologi er relevant at belyse en rapport med netop denne problemstilling. Igennem denne teknologianalyse af VPN-forbindelser forventer vi dog også at belyse andre aspekter af teknologien, som potentielt kan åbne for en diskussion om anvendelsen af VPN. Heriblandt henvises til de førnævnte punkter omkring teknologiens utilsigtede effekter, samt hvordan VPN-teknologien, som et produkt, kan udbredes.

Trin 1: Indre mekanismer & Trin 2: Teknologiens artefakter

Dette afsnit har til formål at identificere de teknologiske artefakter der findes i VPN-teknologien samt at redegøre for disse artefakters indre mekanismer. TRIN-modellens trin 1 og 2 bliver i dette afsnit skrevet sammen, fordi vi mener, det giver bedre mening at identificere artefakterne og redegøre for deres virkemåde, i den rækkefølge, der kommer, i stedet for at adskille VPN-teknologiens artefakter og deres indre mekanismer. Afsnittet starter med en beskrivelse af hvordan netværk fungerer, herunder LAN, local area network, samt WAN, wide area network. Herefter følger en gennemgang af firewall-teknologien og dennes funktion, samt en redegørelse for 2-faktor-godkendelse. Slutteligt afrundes afsnittet med at beskrive kryptografi og en afsøgning af VPN-protokollen PPTP.

Netværk

Et computernetværk er i sin mest basale form en samling specialiseret kommunikationsudstyr, der er indbyrdes forbundet. Hardware, såsom routere, switches og access-points, er fundamentet for ethvert netværk, og det er gennem dette udstyr, muligheden for at skabe et netværk opstår (Cisco1, u.d.). Betragtes et moderne hjemmenetværk, består dette som regel både af computere, mobiltelefoner, printere, fjernsyn og måske endda anden smart teknologi til hjemmet i form af enten støvsugere, kaffemaskiner eller køleskabe. Grunden til, at disse enheder kan kommunikere med hinanden over netværket, skyldes samspillet mellem det førnævnte netværksudstyr (Cisco2, u.d.).

Switches

En switch udgør den simpleste form for et netværk. Det er switchens opgave at forbinde de enheder, der findes på netværket, med hinanden, så de kan kommunikere og udveksle information (Cisco3, u.d.). Når to eller flere enheder er forbundet til en switch, eksempelvis en computer og en printer, er der grundlag for kommunikation herimellem. Ønskes det at printe noget på printeren, må der nødvendigvis kommunikeres fra computeren til printeren, at der kommer et printjob, men også, hvad der skal printes. Det er netop denne kommunikation mellem computer og printer, som switchen varetager (Cisco1, u.d.).

Switchen opererer som udgangspunkt i OSI-modellens lag nummer 2, *data link*, hvilket er en protokol, der forbinder netværksenheder direkte med hinanden – dog kan nogle switches operere i OSI-modellens tredje lag, *network*, hvilket er relevant, når der skal kommunikeres gennem virtuelle netværk (NetworkWorld2, u.d.). Når en enhed forbindes til en switch, identificeres enhedens unikke MAC-, eller 'media access control'-adresse. MAC-adressen kan forstås som en unik, fysisk adresse for en netværksforbundet enhed, og det er denne adresse, switchen bruger, når den skal sende datapakker frem eller tilbage mellem netværksenheder (NetworkWorld1, u.d.). Betragtes eksemplet fra før, med netværket, der indeholdt en computer og en printer, vil der altså kunne findes en MAC-adresse for henholdsvis computeren og printeren, og switchen bruger så disse adresser til at sende datapakken, om at printe noget på printeren, det rigtige sted hen. Når computeren udsender en datapakke, havner den i første omgang hos switchen, hvor datapakkens header bliver læst, og det afgøres, hvor pakken skal sendes hen (NetworkWorld1, u.d.).

Access-points

Switches er typisk kabelbaserede, hvorfor det kan vise sig ganske problematisk at forsøge at tilføje en mobiltelefon, en tablet eller et andet trådløst netværksapparat direkte til en switch. En løsning på dette er access-points. Access-points fungerer på samme måde som switches, blot med den ene forskel, at der kan forbindes uden brug af kabler (Cisco1, u.d.).

Routere

Routere sammenlignes ofte med switches, da de på mange måder udfører samme den samme opgave. Forskellen skal findes i, at routere kan operere i OSI-modellens lag nummer 2, men som udgangspunkt opererer i OSI-modellens lag nummer 3, hvor lag nummer 2 som nævnt er data link direkte mellem to enheder, og lag nummer 3 er *network*-laget (NetworkWorld1, u.d.). Netværksegenskaberne fra OSI-modellens lag nummer 3 gør det muligt for en router at forbinde netværk med andre netværk, og i denne forbindelse også at forbinde enheder på et givent netværk til internettet (Cisco2, u.d.). OSI-modellens lag nummer 3 omfatter funktionalitet, der gør det muligt for routere at forbinde til hinanden og sende datapakker frem og tilbage mellem adskilte netværk. Det er på dette niveau, at *internet protocol*-, eller IP-adresser kommer i spil. Folk

forbinder ofte IP-adresser med internettet, og selvom det er delvis sandt, så er funktionen af IP-adresser blot at angive en adresse, hvortil en datapakke skal sendes (OSI-model, u.d.).

LAN

Local area network, LAN, beskriver et netværk af enheder, der er samlet på det samme geografiske sted. Der lægges vægt på local og dette ords umiddelbare betydning, fordi netværket ikke breder sig udover de funktioner, en switch kan udføre. Der er altså tale om enheder, der, for simplicitetens skyld, ikke kommunikerer med internettet eller andre fjerne netværk (Scott, Wolfe & Erwin, 1998, 1).

Typiske lokalnetværk kan findes i eksempelvis virksomheder eller i private hjem. Tages der udgangspunk i virksomheder, kan det formodes, at der forefindes diverse netværksenheder, såsom servere, computere, printere med videre, på virksomhedens netværk. Lokalnetværket forbinder altså i dette tilfælde disse enheder med hinanden og sørger for, at der kan udveksles datapakker. Lad det antages, at en virksomhed breder sig over to lokationer, og at hver lokation har deres eget lokale netværk. Ifald det bliver nødvendigt for virksomheden at sende information frem og tilbage mellem disse adskilte lokalnetværk, skal der tilføjes en router til hver af lokalnetværkene, så der kan skabes forbindelse udadtil.

WAN

Wide area network, WAN, defineres som sammensætningen af mindst to lokalnetværk. Tages der udgangspunk i eksemplet med virksomheden, der breder sig over to lokationer, bliver de to individuelle netværk først til et WAN, når routerene sender datapakker fra et LAN til det andet (Scott, et al., 1998, 1).

Betragtes et lokalnetværk, og ønskes der at forbindes til dette netværk fra et fjernt netværk, eksempelvis fra et hjemmekontor til en virksomhed, kan der benyttes et *virtual private network*. VPN-forbindelser bruges til at skabe virtuelle forbindelser, i daglig tale kaldet tunneler, mellem lokalnetværk, og til at lave en sikker forbindelse over internettet iblandt disse netværk (Scott, et al., 1998, 2). VPN-forbindelser antages at være sikre, fordi der er nogle indbyggede mekanismer, der

eksempelvis sørger for at kryptere de datapakker, der sendes gennem forbindelsen (Scott, et al., 1998, 1). Virtual private networks er virtuelle, fordi de benytter sig af virtuelle, midlertidige forbindelser, altså ikke-fysiske forbindelser, til at sende datapakker frem og tilbage over internettet (Scott, et al., 1998, 2). Det førnævnte, dagligdags begreb, VPN-tunnel, opstår altså på baggrund af, at der skabes en form for tunnel mellem to adskilte netværk over internettet, og at denne tunnel har til formål at afskærme den datastrøm fra resten af internettet, der findes heri.

Firewall

En central del af VPN-teknologien er firewalls. Firewalls er typisk placeret ved indgangen til et lokalnetværk eller for enden af en VPN-forbindelse, hvorfor al trafik, der skal sendes igennem til netværket, skal passere her (Scot, et al., 1998, 19). En firewall har som udgangspunkt to opgaver at varetage; den første er at kontrollere, hvad en enhed på lokalnetværket kan "se" udadtil, altså på internettet. Den anden opgave handler om at kontrollere, hvad enheder på internettet kan "se" på lokalnetværket, altså inde bag firewallen (Scot, et al., 1998, 20). Der findes forskellige typer firewalls, men der vil i denne sammenhæng kun redegøres for pakkefiltrering firewalltypen.

Pakkefiltrering

Pakkefiltreringsmekanismen er en sikkerhedsanordning, der sørger for, at datapakker, der sendes ind og ud gennem et lokalnetværk, ender de steder, det er dem tiltænkt. For at en datapakke kan få lov til at passere firewallen, skal den opfylde mindst én af de konfigurerede regler, der er sat op for datapakkeoverførsel (Stallings & Brown, 2018, 315). Når en datapakke læses af pakkefiltreringsmekanismen, læses kun datapakkens header og ikke selve den data, der er indlejret i pakken. I headeren findes information om blandt andet, hvilken IP-adresse datapakken kommer fra, og hvilken IP-adresse datapakken skal sendes til. Herudover findes der også information om, hvilke(n) kilde- og destinationsport(e), og endvidere også hvilken transportprotokol, pakken sendes med (Scott, et al., 1998, 20). Filtreringsmekanismen læser headeren for hver datapakke, den støder på, og holder indholdet op mod de opsatte regler, der måtte være for firewallen. En regel kunne eksempelvis være som følger:

En pakke, der har **retningen ind**, som kommer **fra en ekstern IP-adresse**, der skal **sendes til en intern IP-adresse**, som sendes **med TCP-protokol**, på **port 25**, skal have lov til at passere firewallen.

I reglerne, der er konfigureret for firewallen, er det altså forudbestemt, hvilke kriterier en datapakke skal leve op til, for at den kan passere. Antallet af regler, der findes i firewallen, bestemmes af den trafik, der skal tilgå det netværk firewallen beskytter – er der meget varieret trafik, findes der flere regler, end hvis trafikken var ensartet (Stallings & Brown, 2018, 316).

Et problem, der findes ved pakkefiltrering, er, at der ikke er bygget en bruger-autorisationsmekanisme ind sammen med valideringen af de datapakker, der sendes igennem firewallen. Dette betyder, at bruger-autorisation må ske på anden vis, eksempelvis gennem 2-faktor-godkendelse (Scott, et al., 1998, 22-23).

2-Faktor-godkendelse

Begrebet 2-faktor-godkendelse dækker over at 2 faktorer skal opfyldes før noget kan godkendes (Pfleeger, et al., 2015, 68). Autentifikationsfaktorer findes i forskellige udgaver. Viden kan være en autentifikationsfaktor, og denne bruges typisk i sammenhænge, hvor information skal indtastes i login-form. Her anvendes en persons viden om, at vedkommende har et unikt brugernavn og et unikt password, som skal bruges til at logge ind med. Udover viden kan eksempelvis ejendele, placering eller biometri også anvendes som autentifikationsfaktorer. Et eksempel på at anvende ejendele som autentifikationsfaktor kan eksempelvis være, at benytte brugerens mobiltelefon og hertil fremsende en ekstra kode, der skal indtastes i forbindelse med login.

Når der anvendes mere end én enkelt autentifikationsfaktor, sikres det i højere grad, at den person, der prøver at tilgå noget information, faktisk er den person, der må tilgå informationen. Pointen bag, at tilføje et ekstra autentifikationsniveau, er altså at gøre det sværere for uautoriserede at skabe sig adgang til hemmeligholdt information. Ifald en uautoriseret person får opsnappet nogle login-informationer, kan en uautoriseret login-hændelse forhindres, fordi personen ikke er i besiddelse af autentifikationsfaktor nummer to (Pfleeger, et al., 2015, 68-69).

Protokollen PPTP

Point to point tunnelling protocol bygger på indkapsling og kryptering, og det, denne protokol har til opgave, er, at de datapakker, der sendes igennem en VPN-forbindelse, hemmeligholdes og adskilles fra resten af internettet (Scott, et al., 1998, 67). Med indkapslingen menes, at datapakken, der inden indkapslingen har en header med eksempelvis TCP-informationer, pakkes ind i en IP-kapsel, og hermed får en ny ydre header med IP-information. Fordelen ved dette er, at den indkapslede pakke vil blive behandlet som et IP-medium, i stedet for eksempelvis et TCP-medium, og dermed kan sendes over internettet (Scott, et al., 1998, 67).

Ønskes der eksempelvis at oprette forbindelse fra et hjemmekontor til en virksomhed, skal der oprettes en PPTP-tunnel imellem disse. En sådan tunnel oprettes ved at der tages kontakt til virksomhedens RAS-server, 'remote access service'-server, og denne vil forsøge at autentificere personen, der prøver at skabe forbindelsen (Scott, et al., 1998, 67). Hvis forbindelsen verificeres, startes en netværkssession gennem en PPP, point to point protocol, og der kan nu sendes eksempelvis IP-indkapslede TCP-datapakker frem og tilbage i tunnelen mellem hjemmekontoret og virksomheden. Kontinuerligt under hele forbindelsens oppetid, vil der ske autentifikation mellem RAS-server og bruger, samtidig med at datapakkerne bliver krypteret.

Kryptografi

Kryptografi er en central del af VPN-teknologien, og ofte er det netop denne funktion, folk forbinder med VPN-teknologien – nemlig at den datatrafik, der sendes gennem en VPN-forbindelse, bliver krypteret. Hvis PPTP-protokollen anvendes, benyttes MPPE-krypteringsalgoritmen til at kryptere de datapakker, der sendes gennem VPN-forbindelsen (Scott, et al., 1998, 35).

MPPE-algoritmen

MPPE, Microsoft point to point encryption, bruges til at kryptere den PPP-trafik, der opstår, når der oprettes en VPN-forbindelse baseret på PPTP-protokollen. MPPE bygger på Ron Rivest's RC4

krypterings algoritme. RC4 er en ”stream cipher”-algoritme, hvilket vil sige den er bygget op omkring brugen af symmetriske chifferskriftnøgler, der anvendes til at kombinere klartekst med pseudotilfældig chiffertekst (Stallings & Brown, 2018, 642). Når en algoritme benytter symmetriske chifferskriftnøgler, betyder det, at det er den samme nøgle, der krypterer klartekst og dekrypterer chiffertekst (Stallings & Brown, 2018, 628-629).

Algoritmen fungerer ved, at en strøm klartekst krypteres med en strøm af varierende chiffertekstnøgler, der genereres ud fra en hovednøgle (Stallings & Brown, 2018, 644). Klarteksten, der skal krypteres, gennemgås anslag for anslag, indtil der er samlet en bestemt mængde, et bestemt antal bits. Denne samling af klartekst bliver derefter krypteret med den seneste chiffertekstnøgle, der udsendes fra nøglegeneratoren. Chiffertekstnøglerne er pseudotilfældige, idet de alle er udledt fra den samme hovednøgle, og fælles for dem er, at de er meget svære at afkode, hvis ikke hovednøglen er tilgængelig (Stallings & Brown, 2018, 644). Chiffertekstnøglerne kan i RC4 sammenhænge have længder af enten 40 bit, 56 bit eller 128 bit, og jo større chiffertekstnøglen er, jo mere sikker kan krypteringen antages at være.

Trin 3: Utilsigtede effekter

I dette afsnit præsenteres der nogle af VPN-teknologiens utilsigtede effekter. Der er fokus på nogle forskellige aspekter af teknologiens funktionalitet og den tekniske konstruktion og anvendelse, primært i en virksomhedssammenhæng, men vi inkluderer også andre, generelle aspekter. De inkluderede effekter er ikke en udtømmende liste, men rettere en samling af nogle af de mere bemærkelsesværdige sideeffekter.

Netværkets flaskehals

VPN-teknologien er nyttig, hvad angår at tilgå virksomhedens ressourcer i sammenhæng med fjernarbejde. Opkoblingen til arbejdspladsens interne netværk tillader medarbejderen at benytte disse ressourcer, uden at være fysisk til stede på arbejdspladsen. Normalvis fungerer en sådan VPN-forbindelse på den måde, at der etableres en tunnel fra den hjemmearbejdende ansatte til arbejdspladsens lokalnetværk, hvor trafikken mellem bruger og netværk overvåges. Knudepunktet for interaktionen mellem serverens ressourcer og den hjemmearbejdende ansatte er adgangsporten til virksomhedens lokalnetværk, en adgangsport, der har til funktion at processere og dekryptere datapakker. I perioder med mange aktive VPN-forbindelser fra hjemmearbejdende ansatte betyder dette imidlertid, at adgangsportens evne til at processere informationen fra medarbejderne vil komme under pres, og denne systembelastning kan resultere i nedsat effektivitet og mere ventetid fra medarbejderens position, idet alle fjernforbindelserne skal gå igennem denne port (Jeffery, 2020).

Når en bruger er forbundet til en fjernserver via en VPN-forbindelse, betyder dette også, at deres adgang til det offentlige internet foregår igennem fjernserveren og ikke direkte igennem deres eget, lokale netværk. Hos virksomheder betyder dette normalvis, at al trafikken igennem fjernnetværket overvåges. Dette betyder imidlertid mere pres på VPN-forbindelsen, når brugeren er forbundet til fjernnetværket og tilgår internettet igennem dette, selv til ting, der ikke nødvendigvis er arbejdsrelaterede. Dette kan imidlertid mitigeres, ved at gøre brugerne opmærksomme på, kun benytte VPN-forbindelsen, når det er nødvendigt, og at huske at logge af fjernnetværket, når de er færdige med at foretage handlinger, der kræver adgang til fjernserverens ressourcer.

Split-Tunnelling

En anden løsning til systembelastningen er en split-tunnelling-protokol, som opdeler adgangen i interne fjernnetværksressourcer og godkendte, eksterne internetressourcer. Løsningen sørger for, at VPN-forbindelsen kun benyttes til at tilgå fjernnetværkets elementer, således at anden internetinteraktion foregår gennem en anden, mindre ressource- og omkostningstung tunnel. En sådan split-tunnel kan opsættes på forskellige måder, alt efter virksomhedens behov for og afhængighed af eksterne internetressourcer. De to gængse protokoller er *split-include* og *split-exclude*, der hver især forholder sig til, hvordan den passerende trafik skal filtreres. Split-include er den mere begrænsende variant, der kun tillader adgang til domæner, tilladt af virksomheden. Split-exclude fungerer omvendt og tillader friere tilgang til domæner med blokering af specifikke, blacklistede domæner. Dette kan spare på ressourcerne hos fjernnetværket og reducere systembelastning (Jeffery, 2020).

Dog betyder dette også, at eventuelle sikkerhedsfiltre, der benyttes på fjernnetværket, også omgås, hvilket kan have alvorlige konsekvenser, hvis brugerens system inficeres med malware eller bliver kompromitteret af hackere. I sådanne tilfælde vil disse cyberkriminelle muligvis kunne bryde ind i virksomhedens systemer igennem brugerens VPN-forbindelse til fjernserveren (Jeffery, 2020). I denne sammenhæng er en VPN-forbindelses sikkerheds- og krypteringsteknologier ikke til megen nytte, idet disse sikkerhedselementer først træder i kraft, når tunnelen er oprettet, og derfor ikke strækker sig over selve værtssystemets forhold. Løsninger til den lokale sikkerhed kan for eksempel være anvendelsen af to-faktor-godkendelsesløsninger eller øget agtpågivenhed mod maliciøse indtrængningsmetoder, såsom phishing eller målrettede spear-phishings (Bilag 2).

IPv6-Breakout

Internettets primære funktion er overførslen af informationer fra et sted til et andet, og dette kan lade sig gøre på grund af internet protokoller (IP). IP er et standardiseret regelsæt, hvis funktion er at homogenisere det digitale informationsudvekslingsnetværk, således at kommunikation over internettet er så effektivt som muligt. Alle noder i et netværk, såsom computere eller routere, bliver tildelt en IP-adresse til kommunikation herimellem.

På nuværende tidspunkt er den fjerde version af internetprotokollen, bedre kendt som IPv4, den mest udbredte version, og den dækker over mere end 4 milliarder unikke IP-adresser, hvoraf mange er allokeret til specielle formål, og dermed ikke er tilgængelige for normal IP-adressetildeling. Denne begrænsede mængde af ledige IPv4-adresser betyder imidlertid, at der snart ikke er flere tilgængelige IPv4-adresser. Den nyeste version af internetprotokollen, IPv6, er tiltænkt at skulle erstatte IPv4 med et markant højere antal ledige adresser, og IPv6 er så småt i gang med at blive rullet ud på verdensplan.

Overgangsperioden fra IPv4 til IPv6 er ikke en gnidningsfri proces, og det samme gælder konverteringen af VPN-teknologien fra IPv4 til IPv6. Terminologien *IPv6 VPN Breakout* refererer til, hvordan VPN-services er konfigureret i forhold til internetprotokollerne, og hvordan mange af disse services muligvis ikke er kompatible med den nye IPv6-standard. Dette betyder, at hvis den givne VPN-konfiguration kun er indstillet til at bearbejde datapakker baseret på IPv4-protokollen, og en bruger anvender IPv6-protokollen, har alle de intenderede sikkerhedsforanstaltninger, der burde appliceres, ikke nogen effekt. Resultatet af dette er, at datapakker baseret på IPv6 kan passere frit igennem og tilgå det offentlige internet igennem fjernetværket (Hogg, 2019).

Et IPv6 VPN-breakout forekommer primært hos virksomheder, der benytter sig af no split-tunnelling, hvilket betyder, at al kommunikation fra brugerens enhed passerer igennem VPN-fjernserveren til inspektion og eventuel blokering af uønsket trafik (Hogg, 2019). Heri er det normen at konfigurere IPv4 som standardprotokol og ofte udelukke eller helt at glemme også at konfigurere IPv6-protokollen, idet denne protokol stadig er i de tidlige stadier af udrulning (Hogg, 2019).

I takt med den stigende optagelse af IPv6-adresser og IPv6-parate enheder hos brugere på internettet, vil det i højere grad blive nødvendigt for virksomheder at tage stilling til dette fænomen. Der eksisterer effektive løsninger på problemstillingen, såsom at opdatere virksomhedens lokalnetværk til at understøtte IPv6-protokollen, og i samme dur opdatere konfigurationen af VPN-forbindelsen til at inkludere IPv6-interaktioner (Hogg, 2019).

En anden løsning er at inkorporere DNS (Domain Name System), en slags telefonbog over domænenavne, direkte i processen, og dermed tvinge tilbageholdelsen af IPv6-anmodninger og kun tillade IPv4. Dette betyder imidlertid, at eventuelle IPv6-applikationer vil opleve stærkt reduceret effektivitet, idet forbindelsen slår fejl og falder tilbage til IPv4-protokollen (Hogg, 2019).

Anonymitet og cyberkriminalitet

Især i nyere tid er markedet for kommercielle VPN-services vokset eksplosivt. Der reklameres for personlig anonymisering af det digitale fodaftryk, og frihed til at færdes på internettet uden at bekymre sig om, hvilke tredjeparter, der ser med. Som udgangspunkt er disse VPN-services markedsført på sociale medier som redskaber til at opretholde brugerens anonymitet og sikkerhed på internettet. Ydermere loves det, at de kan give mere fleksibilitet i forhold til geografisk lokationsdata, som for eksempel at få adgang til en streamingtjenestes indhold i andre lande, eller at gøre sin færden på det offentlige internet mindre synlig, og desuden modvirke internetudbyderes indsamling og salg af brugerinformationer til tredjeparter (Larsson, Svensson, de Kaminski, Rönkkö, & Olsson, 2012, 263).

Men denne digitale anonymitet åbner også døren for ”alternative” anvendelsesmetoder. Cyberkriminalitet findes i mange forskellige former og størrelser. En af de mere udbredte, kriminelle aktiviteter, der ofte benytter sig af VPN-teknologien, er for eksempel piratkopiering af digitale medier, og ikke-licenseret, online fildeling. Heri benyttes VPN-teknologiens evne som et værktøj til at sløre identitet og geografisk lokation, og til at skjule personers digitale fodaftryk på internettet, således at disse i højere grad kan undgå at blive identificeret af myndighederne, og dermed undvige juridiske konsekvenser (Larsson, et al., 2012, 261).
En undersøgelse foretaget af Larsson et al. (2012) havde til formål at undersøge anvendelsen af VPN-services eller lignende teknologier hos anonyme brugere på fildelingshjemmesiden *The Pirate Bay* i forbindelse med deres færden på og interaktioner med hjemmesidens indhold. Undersøgelsen viste, at 17,8% ud af undersøgelsens 75.000 deltagere anvendte VPN-services, når de benyttede sig af fildelingshjemmesiden, og at det især var de mere aktive brugere, der uploadede indhold, som benyttede VPN-services til at anonymisere sig bag (Larsson, et al., 2012, 273).

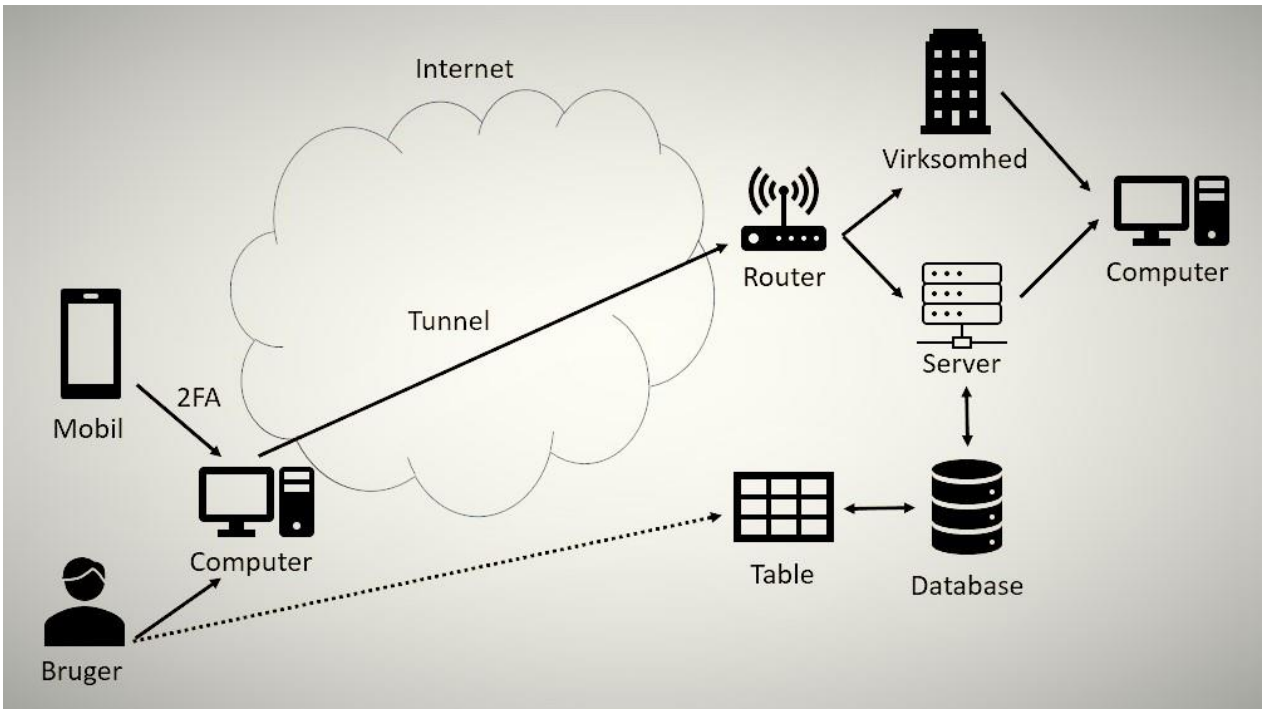
Trin 4: Teknologiske systemer & Trin 5: Modeller

I denne del af trinmodellen har vi valgt slå trin 4 og 5 sammen. Dette betyder, at der kommer til at være modeller af de teknologiske systemer, hvori VPN-teknologien indgår. Det ville være tilstrækkeligt at beskrive systemerne, men modellerne giver en bedre og mere visuel forståelse.

VPN-teknologien kan beskrives i mange forskellige teknologiske sammenhænge. Vi kigger i denne rapport på, hvordan teknologien bliver brugt i forbindelse med, at danske medarbejdere skulle arbejde hjemmefra. Dette perspektiv giver os særligt to teknologiske systemer, der er relevante at kortlægge og undersøge. Både det system, som overordnet set kan karakteriseres som værende det lokale netværk på hjemmekontorerne, men også det generelle system, hvori VPN-teknologien kan betegnes som værende et teknologisk system i sig selv. Sidstnævnte system handler om, hvordan der kan skabes forbindelse mellem en medarbejders computer på hjemmekontoret og virksomhedens netværk. Vi vil i dette afsnit starte med at kortlægge VPN-teknologiens generelle system og derefter kortlægge og undersøge, hvordan teknologien hænger sammen med hjemmekontoret (Jørgensen, 2018). For at give en bedre forståelse af vigtigheden af systemerne, vil disse kortlægninger også indeholde modeller, lavet af gruppen, som tydeliggør de teknologiske systemer.

VPN-teknologien som teknologisk system

VPN-teknologien kan betegnes som værende et teknologisk system i sig selv. Det er et system mellem menneskelige aktører, internettet, teknologiske artefakter og en organisation med et netværk. De menneskelige aktører er brugere, som skal tilgå et netværk via fjernadgang. Organisationen er den, som har det netværk, brugeren forsøger at tilgå. De teknologiske artefakter vil oftest være computere, internet-routere og servere hos organisationen. Internettet kan i dette tilfælde beskrives som værende måden, hvorpå de førnævnte kan kommunikere med hinanden. Dette sker gennem protokoller, som på forhånd er aftalt mellem brugere, artefakter og organisationer. Disse protokoller gør, at brugeren kan genkendes på organisationens netværk og derved kan åbne en forbindelse dertil.



Figur 3 [Model over det generelle teknologiske system der er VPN-teknologien]

Ovenstående model viser det teknologiske system, VPN-teknologien er. En bruger logger på sin computer og forbinder sig til virksomhedens netværk gennem sin router. For at kunne oprette denne forbindelse vil brugeren i nogle tilfælde modtage en to-faktor-godkendelse (2FA) på sin telefon. Når en bruger logger på, tjekkes loginforsøget mod en database, som ligger på en af virksomhedens servere eller enheder. Denne interaktion styres ofte af virksomhedens Active Directory, som er en Windows-mekanisme, der administrer brugeradgang. Hvis brugeren genkendes, kan vedkommende nu få adgang til enheder på virksomhedens netværk. Forbindelsen, som oprettes, kaldes *tunnelling*, tillader sikker kommunikation mellem brugens computer og virksomhedens netværk ved brug af *layering*, indkapsling og kryptering (Welekwe, 2021).

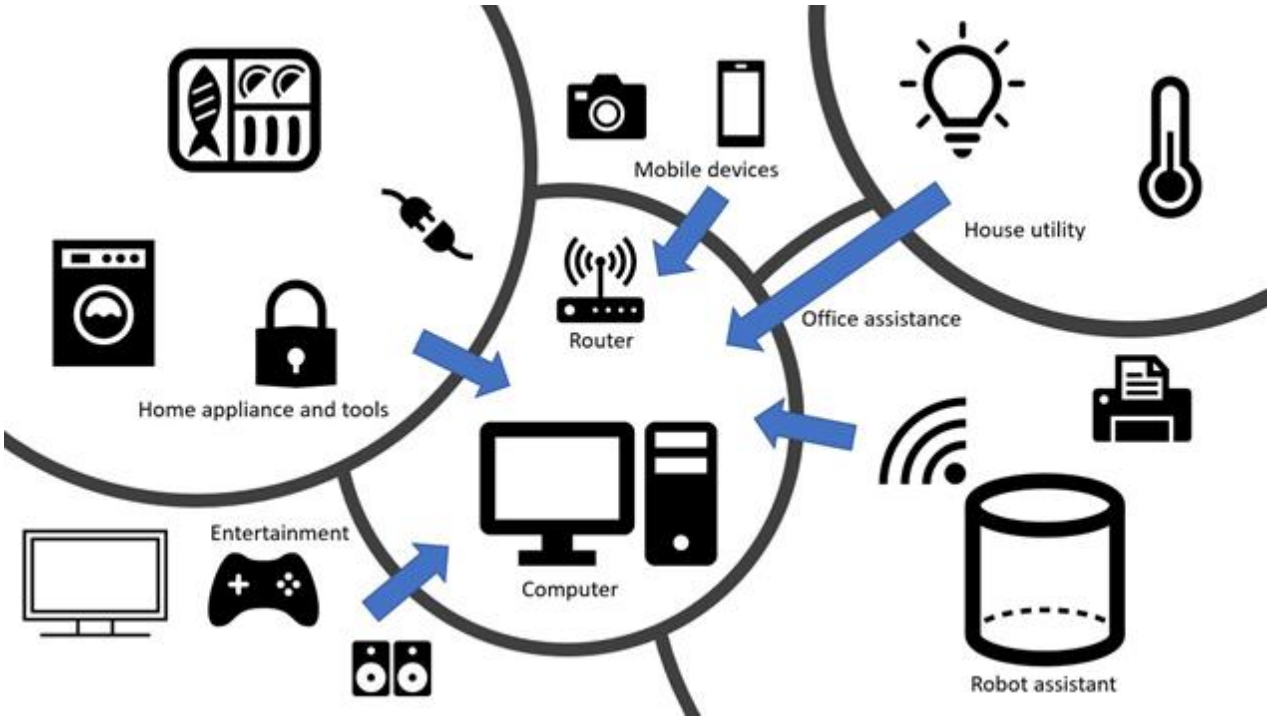
Årsagen til, at dette system er vigtigt at kortlægge og visualisere, er, at det tydeliggøres, hvordan der med omstillingen til hjemmekontorer også er kommet en del flere steder, hvor datatilgængelig kan udfordres. Der er med omstillingen kommet flere led i den forbindelse, der kræves for at tilgå virksomhedens data. Eksempelvis kan der være problemer med både internettet hos brugeren og hos virksomheden, som gør, at en forbindelse ikke kan etableres. Ligeledes kan der eksistere

problemer med udbyderen af den VPN-løsning, virksomheden benytter. Alle disse problemer relaterer sig til COVID-19-omstillingen, og var, forud for denne, ikke aktuel på samme måde.
En anden årsag til, at systemet er vigtigt at kortlægge, er, at det belyser, hvordan brugerens enhed på det netværk, vedkommende arbejder på, får adgang til enheder på virksomhedens netværk. Det er særligt dette forhold, som skaber sikkerhedsproblemerne ved teknologien, hvorfor systemet er vigtigt at forstå. Det er altså ikke selve forbindelsen over internettet, der er betydeligt udsat. I stedet er det det faktum, at brugerens enhed kan være kompromitteret, og at den derved kan agere som bagdør for digitale slyngler. En anden grund til, at denne sammenhæng er relevant at nævne, er, at det giver en forståelse for, at der er en maskine i den anden enden af den forbindelse, brugeren opretter. Dette er en viden, som godt kan overses og derved skabe kompilationer.

VPN-teknologien på hjemmekontorer

VPN-teknologien kan i forbindelse med dette projekt også beskrives i et andet teknologisk system, nemlig det lokale netværk, der eksempelvis findes på et hjemmekontor. Danmark er et af Europas mest digitaliserede lande, og det gælder også, hvad vores hjem angår (Danmarks Statistik, 2021). Det er ikke længere science fiction at have en robot i hjemmet, som kan tale med en og undersøge ting på internettet, mens man taler med den. Disse digitaliserede hjem lader til at være i fremgang, og i takt med at vores hjem og kontorer bliver smartere og smartere, kan det også være relevant at stoppe op og kortlægge, hvordan det hele hænger sammen.

Typisk vil de danske hjemmekontorer have en række teknologiske artefakter forbundet til det samme netværk, som bruges til at forbinde til virksomhedens netværk, når den ansatte arbejder hjemmefra. De mest udbredte enheder er ting som printere, robot-assistenter, fjernsyn og højtalere. Men det kan også være ting så små som en vandpumpe i et akvarie eller en fugtighedsmåler. Alle disse enheder beskrives som at være Internet of Things (IoT), og de er vigtige at betragte som værende en del af ens teknologiske netværk. IoT'er kan nemlig agere som end points for hackere, altså steder, hvor digitale kriminelle kan tilgå hele ens netværk, hvis blot én enhed ikke er ordentligt beskyttet (Tripathy et al, 2018, 219-223).



Figur 4 [Model over teknologier, som forbinder sig til det netværk, der anvender VPN-teknologien]

Figur 4 viser, hvordan et hjemmenetværk kan se ud. Flere og flere apparater i hjemmet bliver forbundet til netværket på en sådan måde, at de kan styres fra mobile enheder eller fra computeren. Det er vigtigt at forstå, at jo flere ting, der implementeres på det samme netværk, jo flere muligheder er der også for, at en hacker kan trænge ind på dette netværk. Her kan det nævnes, at mange af disse apparater har forholdsvis gode, indbyggede sikkerhedsmekanismer, men at det kan være en udfordring at finde og holde øje med de eventuelle svagheder. Det er særligt ældre apparater, der ikke modtager regulære software opdateringer, som kan agere bagdør for en hacker.

Trin 6: Drivkræfter og barrierer ved udbredelsen af VPN-teknologi

Hvad angår materialet, anvendt til at etablere, hvad trin 6's definition på en teknologis drivkræfter og barrierer er, har Jørgensen (2014) taget udgangspunkt i Everett M. Rogers "Diffusion of Innovations" (2003). Derfor vil det følgende analyseafsnit om drivkræfter og barrierer for udbredelse af VPN-teknologien som innovation udføres på baggrund af denne bog.

Ved teorien om diffusion of innovations, er der tale om en diffusion – *kommunikationsproces* – i et socialt system, hvori en bestemt innovation bliver omtalt som en ny idé. I processen udveksler de kommunikerende parter information omkring den nye idé, hvorudfra begge parter udvikler en ny forståelse af idéen. Den usikkerhed, der er omkring den nye idé, er derfor en faktor for, hvorfor kommunikationsprocessen er så vigtig, da informationsudvekslingen kan give de to parter helt nye og potentielt radikalt anderledes indtryk af, hvilke problemer og behov, innovationen søger at løse (Rogers, 2003, 5-6).

> *" Diffusion is the process by which (1) an innovation (2) is communicated through certain channels (3) over time (4) among members of a social system"*
>
> (Rogers, 2003 11)

Dette citat søger at definere essensen af en diffusion, og, som markeret, inddele denne proces i de fire elementer. I de følgende afsnit vil vi undersøge, hvad disse fire elementer betyder for diffusionen af en VPN. Det skal desuden nævnes, at eksempler på sociale systemer kan fortolkes i forskelligt omfang, men den strukturelle komposition, som Rogers definerer, kan ligeledes anvendes til organisationer og strukturen heri (Rogers, 2003, 402-403). Eftersom denne rapport søger at besvare, hvilke IT-sikkerhedsmæssige problemstillinger virksomheder har mødt ved at omstille medarbejdere til hjemmekontorer, anvendes denne teori med et organisatorisk standpunkt, hvorfor vi fremadrettet vil betragte et socialt system som en organisation.

Rogers beskriver **innovation**, i et teknologisk aspekt, som bestående af en *hardware*, forstået som det produkt, innovationen er, og en *software*, forstået som viden til at bruge produktet (Rogers,

2003, 36). Hardware- og softwarebegreberne bliver her anvendt på utraditionel vis, eftersom en VPN-forbindelse for eksempel, ifølge Rogers, beskrives som en hardware. Innovationens karakteristika, der determinerer, hvor hurtigt den udbredes, kan undersøges ud fra de fem nedenstående aspekter:

Relative advantage – hvordan innovationen umiddelbart betragtes som værende bedre end konkurrencen eller forgængeren, og blandt andet måles ud fra social prestige, investeringspotentiale eller økonomisk fordel (Rogers, 2003, 15). En VPN-teknologi i en virksomhed tjener først og fremmest det formål at beskytte virksomhedens data, kommunikationen imellem personale og håndtering af data. Dette sker ved at sætte en krypteret linje op imellem medarbejderes computer og virksomhedens server, og dermed omdirigere internettrafikken ud igennem virksomhedens internetforbindelse i stedet for via omkringværende alternativer, såsom medarbejderens Wi-Fi i hjemmet. Det innovative aspekt er derved et sikkerhedsniveau, der kan indføres ved en teknologisk implementering, snarere end ved adfærdsændrende kurser (Bilag 1).

Compatibility – hvordan innovationen er genkendelig i forhold til eksisterende værdier og behov (Rogers, 2003, 15). Ud fra dette aspekt tjener VPN-teknologien brugerens formål om at beskytte egne data og bestræbelsen på, at udefrakommende og fremmede brugere ikke kan følge med i private interaktioner. Set fra et virksomhedsperspektiv betyder dette, at teknologien søger at dække eksisterende behov ved at sikre al data, virksomheden er i besiddelse af, og derudover også den kommunikation og udveksling af data, som sker i virksomheden, lokalt eller hjemme hos de ansatte. Ved at etablere et lukket netværk kan en VPN-forbindelse forebygge uønsket observation af kommunikation internt mellem medarbejdere, hvilket øger trygheden, når der håndteres følsom data (Bilag 1).

Complexity – hastigheden på udbredelsen varierer, afhængigt af, hvor nemt det er at tage innovationen i brug. Hvis idéen indeholder kompliceret eller hidtil ukendt information, er udbredelsen langsommere, end hvis den har et intuitivt design (Rogers, 2003, 16).

Trialability – muligheden, individer har for at afprøve innovationen, inden beslutningen tages om at adaptere eller ej (Rogers, 2003, 16). Hvis afgørelsen af adaptionen af en ny idé afhænger af muligheden for at afprøve den i en specificeret kontekst, kan VPN-teknologien indledningsvist implementeres i en virksomhed i et nedskaleret omfang. Som udgangspunkt kan den digitale adfærd forblive den samme i en virksomhed, der ikke anvender en VPN-forbindelse, hvor enten en enkelt afdeling eller få medarbejdere i en periode opnår adgang til virksomhedens data igennem en VPN. Alt efter, hvordan omstillingen i personalets digitale adfærdsændring udvikler sig, kan ledelsen derfra vælge at afvise eller adaptere VPN-teknologien til alle virksomhedens ansatte.

Observability – når et individs adaption af innovationen tydeligt kan ses af andre og dermed kan udbredes hurtigere (Rogers, 2003, 16). I et dagligt anvendelsesregi ses anvendelsen af VPN-teknologi sjældent af andre individer end brugeren. VPN-forbindelsen sker igennem hardware, der enten er individets personlige eller er suppleret af virksomheden, og foregår i et arbejdsrelateret regi, hvorfor observerbarheden af innovationens anvendelse sjældent ses af andre individer. Det samme kan til en vis grad oversættes til et virksomhedsledelsesperspektiv, hvor observerbarheden af VPN-anvendelsen skal ses som en sikkerhedsstrategi, og hvor denne sker indbyrdes iblandt virksomhedens samarbejdspartnere eller andre tilknyttede aktører.

Kommunikationskanalerne, der nævnes, er det medie, informationen bliver formidlet igennem. Der kan enten være tale om et massemedie eller sociale medier, hvis platforme bidrager til en generel forståelse for og viden om, hvad innovation kan levere. Alternativt kan de mellemmenneskelige kanaler være et informationsmedie, hvori individer kan dele deres personlige erfaringer, indtryk og information i en dialog, der fører til en beslutning om at adaptere innovationen eller ej. De interpersonelle kanaler ses ofte imellem individer, som lever efter forskellige overbevisninger, men mødes om den fællesnævner, innovationen er. Derved agerer individerne gensidige rollemodeller og bliver inspireret af informationsdelingen i kommunikationskanalen (Rogers, 2003, 36). I scenariet om virksomheders adaption af VPN-teknologien vil enkelte kommunikationskanaler have potentiel indflydelse på virksomhedens adaptionsbeslutning. En mulighed kan være, at VPN-udbyderen allerede har virksomheden som

kunde på andre produkter, såsom firewall eller anden software, hvorfor de kan promovere deres VPN-innovation til virksomheden, der derved allerede har et forhold til VPN-producenten (Bilag 1). En anden mulighed kan være et samarbejde på tværs af flere virksomheder, hvor individerne blandt andet kan dele deres erfaring og indtryk om VPN-teknologien med hinanden. De kan mødes i varierende virksomhedssammenhænge, men mødes om at have et behov for at beskytte deres data og håndteringen heraf.

Tiden, det tager innovationen at udbredes til individer, er afhængig af en proces, der strækker sig over fem dele:

Knowledge – den information, individet tilegner sig om innovationen og dens formål (Rogers, 2003, 20). For at en VPN-teknologi skal kunne udrulles til målgruppen, i dette projekt virksomheder, kræver det i første omgang, at virksomheden skal danne kendskab til teknologien og have information herom. Jo mere målrettet, den kommunikationskanal, som information om VPN-teknologien bliver formidlet igennem, er, jo hurtigere stifter virksomheden bekendtskab med, at denne VPN-teknologi eksisterer på markedet, samt hvordan den adskiller sig fra konkurrerende produkter, og hvilke behov den søger at dække.

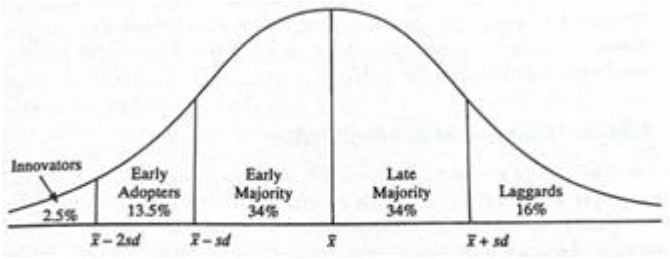
Persuasion – det forhold, som individet danner til innovationen. Dette kan være et positivt, negativt eller kritisk forhold (Rogers, 2003, 20).

Decision – individets beslutning om at adaptere innovationen eller ej (Rogers, 2003, 20). Når information om VPN-teknologiens eksistens har nået virksomheden, er det herfra op til virksomheden, hvorvidt innovationen skal adapteres eller ej; en beslutning, der træffes ud fra, om den lever op til virksomhedens forventninger til og kriterier for beskyttelse af virksomhedens data. Det er blandt andet de fire førnævnte begreber, *relative advantage*, *compatability*, *trialability* og *observability*, der er afgørende for, hvorvidt en virksomhed vælger at adaptere eller ej.

Implementation – når individet tager innovationen i brug, og danner sig nye indtryk heraf (Rogers, 2003, 20). Hvis virksomheden herefter vælger at adaptere og implementere VPN-innovationen, kan

dens anvendelse afvige fra den oprindeligt tiltænkte funktion, der blev kommunikeret ud i *knowledge*-fasen.

Confirmation – er en bekræftelse på, at beslutningen om at adaptere innovationen var korrekt (Rogers, 2003, 20).



(Figur 5 Rogers, 2003, 281)

Figuren beskriver, hvor i udbredelsesprocessen innovationen er nået til, og hvor stor en andel af brugere, der kategoriseres inden for hver type. Den første type, *innovators*, er individer, der har stor interesse i nye innovationer og i nytænkning af idéer. Det er disse, der først adapterer og videredeler information om innovationen; de næste tre typer, *early adopters, early majority* og *late majority*, er mere tøvende og kritiske over for nye idéer og afventer et bevis på, at innovationen opfylder det tiltænkte formål. Den sidste type, *laggards*, er traditionalisterne, der har svært ved at lade sig overtale af nye idéer (Rogers, 2003, 282-284). I forhold til udbredelsen af en VPN-løsning, så kan virksomhedstypen give et fingerpeg om adaptionstypen. For eksempel, hvis den virksomhed, der skal adaptere, sælger IT-produkter og har et IT-strategisk mindset, kan virksomheden sandsynligvis være tilbøjelig til at adaptere VPN-innovationen tidligt – *innovator* – hvorimod ikke- eller kun delvist digitaliserede virksomheder kan være forbeholdne over for at adoptere innovationen – *laggards.* Derudover findes naturligvis de virksomheder, der ikke nødvendigvis promoverer sig selv som en IT-virksomhed, men ved, hvad de er værd i data og digitalisering.

Det sidste element i diffusionsprocessen omhandler det **sociale system**, som kommunikationen om innovationen indgår i. Et socialt system skal forstås som et fællesskab, der søger at løse det samme problem, og har en struktur, et normsæt, samt et individhierarki, hvor nogle kan have

mere indflydelse på innovationsadapteringsbeslutninger end andre. Beslutningen om at adaptere en innovation varierer for hvert socialt system, og det kan enten være en fri, individuel beslutning, en kollektiv beslutning, eller det kan være en autoritetsbeslutning, hvis det sociale system har en bestemmende autoritet (Rogers, 2003, 37-38). I forhold til adaptionen af en VPN-forbindelse i en virksomhed, er der her tale om en autoritetsbeslutning i det sociale system, eftersom det er en virksomhedsledelse, der determinerer, hvorvidt denne teknologi skal tages i brug på arbejdspladsen. Når først denne beslutning tages og implementeres, udvikles virksomhedens digitale adfærd og sikkerhedsforanstaltninger efter VPN-innovationen. Det vil sige, at der sker en tvungen adaption af VPN-teknologien for samtlige ansatte, eftersom denne forbindelse er obligatorisk for, at medarbejderen kan tilgå virksomhedens data.

For at opsummere, hvilke drivkræfter, der ses ved udbredelsen af VPN-teknologien i virksomheder, er drivkræfterne innovationens evne til at beskytte virksomhedens data, samt intern kommunikation imellem personale, heriblandt også den datahåndtering, der finder sted i kommunikationsprocessen. Derudover er VPN-teknologien en supplerende teknologi, hvad angår virksomheden og dets IT-personales indførelse af en sikkerhedsstrategi til hjemmearbejdende. Dette kan bidrage som sikkerhedsnet i tilfælde af, at virksomhedens personale ikke er undervist i sikker digital færden. Ved omstillingen til hjemmekontor kan der desuden argumenteres for, at der er en arbejdskraftmæssig fordel i at investere i en VPN-licens til hjemmearbejdende ansatte. Dette medfører, at medarbejderen på relativ kort tid kan påbegynde sit arbejde i stedet for at bruge tiden på kurser om sikkerhed ved omstilling, hvis undervisning heri ikke allerede har fundet sted. Af barrierer for udbredelsen af VPN-teknologien, ligger der en fundamental uvished om, hvordan implementeringen af VPN-innovationen påvirker personalets arbejdsgang. Hvis den sikkerhedsprotokol, VPN-teknologien medfører, har mange sikkerheds-check-points, kan det risikere at forstyrre de enkelte, ansatte individers flow of work. Dette kan potentielt medføre et negativt forhold mellem bruger og VPN-teknologi, men individerne er alligevel tvunget til at anvende VPN-forbindelsen, eftersom adaptionsbeslutningen er truffet af virksomhedsledelsen i et autoritært socialt system. Der er altså her tale om potentielle komplikationer med sikkerhedens tilgængelighed.

Analyse

Hvilke problemstillinger har der været i forbindelse med omstillingen?

Omstilling til hjemmekontorer betyder, at de hjemmearbejdende skulle have adgang til arbejdspladsens ressourcer hjemmefra. Anvendelsen af VPN-løsninger er ikke et nyt fænomen, og store virksomheder har draget nytte af denne teknologi i flere årtier, dog ikke i samme størrelsesorden som netop nu. Hjemsendelsen af virksomheders ansatte i sammenhæng med COVID-19-pandemien har øget fokus på, hvordan disse kan fortsætte deres arbejde uden den direkte adgang til virksomhedens ressourcer. Dette inkluderer aspekter som benyttelsen af virksomhedens teknologiske løsninger, tilgang til filer på servere, ændringen af arbejdsgange og adfærd, samt hvilke konsekvenser, der kan forekomme, når det fysiske fremmøde og samarbejde ikke er en mulighed. Udover de interne faktorer, har omstillingen til hjemmekontorer også medført en række problematikker fra virksomhedens eksterne ressourcer, såsom tekniske løsninger fra tredjepartsvirksomheder.

VPN-flaskehalsen

En af de tekniske problemstillinger, der forekom i sammenhæng med hjemsendelsen af medarbejdere og anvendelsen af VPN-teknologien hos virksomheder, var båndbreddemæssige flaskehalse. Disse flaskehalse opstår, når der etableres mange forbindelser til virksomhedens netværk igennem VPN-forbindelse, og alle disse interaktioner skal tilgå ressourcer og internetservice via virksomhedens netværk. Selve flaskehalsen opstår, idet alle disse forbindelser undergår diverse sikkerhedstjek, når trafikken foregår igennem VPN-forbindelsen.
Normalvis er systembelastningen for VPN-forbindelser ikke et stort problem, om et problem overhovedet, og forbindelsen var tænkt som en mere fleksibel måde at tilgå virksomhedens ressourcer på, uden altid at skulle befinde sig fysisk på arbejdspladsen.

”Folk har kunnet arbejde hjemme. Nogle gør det aldrig, nogle en gang om måneden, nogle måske en gang om ugen. Det har været meget fleksibelt, og det har alle løsningerne sagtens kunne klare båndbreddemæssigt. Og pludselig var alle hjemsendt, og alle skulle på via VPN på én gang.”

(*Bilag 1*)

Resultatet af disse flaskehalse i VPN-forbindelsen er en langsommere forbindelse til virksomhedens netværk og ressourcer for de ansatte, og jo flere, der skal tilgå disse, jo langsommere bliver forbindelsen (Bilag 4 & Bilag 5). En af de løsninger, der benyttes af mange virksomheder, som benytter VPN-forbindelser til fjernarbejde, er opdelingen af den udefrakommende trafik. Split-tunnelling er en teknik indenfor VPN-teknologien, der tillader VPN-værten, som regel en virksomhed, at konfigurere, hvilken trafik, der skal foregå igennem VPN-forbindelsen, og hvilken trafik, det er acceptabelt at lede udenom.

> *"Så, hvis man for eksempel fravælger trafik, hvor man stoler på, det er tilstrækkeligt beskyttet i forvejen i de applikationer, det foregår i, og som er meget trafiktunge - det kunne for eksempel være Microsoft Teams, især med videostreaming på - så kan man bare 'tunnelle' den ud, så den ikke kører som en del af VPN-løsningen, men bare kører direkte."*

(*Bilag 1*)

Benyttelsen af split-tunnelling til at spare på båndbredden er en effektiv måde at kontrollere trafikken på og mitigere de hastighedsreducerende bivirkninger, der kan forekomme, når der er mange på forbindelsen samtidigt. Men opdelingen af trafikken betyder også, at diverse sikkerhedsprotokoller ikke appliceres til den omdirigerede trafik, og i denne sammenhæng skal det fra virksomhedens side overvejes, hvordan denne trafik kan sikres. Primært er den omdirigerede trafik bestående af internetressourcer, såsom adgang til diverse cloud-løsninger for eksempel Microsoft Office 365, og heri kan virksomheden tage beslutningen om, hvorvidt den eksterne ressources egne sikkerhedsforanstaltninger er tilstrækkelige.

"Med HTTPS, der er det den, du snakker med i den anden ende … Microsoft for eksempel, har vi måske en antagelse om, at de måske er gode nok, men der kan være mange andre leverandører, som måske ikke engang har HTTPS."

(*Bilag 1*)

Omstændigheder som disse har normalvis kun været under overvejelse i de mest ekstreme tilfælde, men hjemsendelsen af majoriteten af virksomheders ansatte har gjort håndteringen af trafikken igennem VPN-forbindelsen til en prioritet. I forbindelse med omstilling til hjemmekontorer er der blevet foretaget et skift fra at benytte VPN-forbindelsen uden restriktioner, til at skulle teste og implementere nye løsninger.

"Det har man ikke gjort tidligere, fordi der var jo båndbredde nok, så der kører vi bare det hele igennem VPN."

(*Bilag 1*)

"… og pludselig var alle hjemsendt, og alle skulle på via VPN på én gang. Og det var ikke testet, det scenarie, før."

(*Bilag 1*)

Fysiske knudepunkter

I takt med at størstedelen af virksomheders ansatte skulle benytte sig af VPN-løsninger for at fortsætte deres arbejde, er det ikke kun de interne faktorer indenfor selve virksomheden, der kan volde problemer. Et kritisk aspekt af arbejdet fra hjemmekontoret via VPN-forbindelsen er den fysiske forbindelse til virksomhedens netværk via internetkabler.

"I min forrige virksomhed, der havde vi et tilfælde: helt lavpraktisk lavede TDC noget gravearbejde, og de gravede nogle af deres egne kabler over, og så havde vi ikke nogen internetforbindelse til kontoret i en periode på i hvert fald to døgn. Vi skulle ikke bruge så meget inde på kontoret, men VPN-linjen kørte derind igennem, så lige pludselig sad der 1000 mennesker, der ikke kunne arbejde."

(*Bilag 1*)

Normalvis ville en manglende internetforbindelse som i dette tilfælde ikke være katastrofalt, idet det interne netværk stadig ville være funktionelt og tilgængeligt for ansatte, der var fysisk til stede i virksomhedens bygninger, og samtidig ville antallet af fremmødte ansatte, der var afhængige af VPN-forbindelsen, være stærkt begrænset. Men den storstilede hjemsendelse af ansatte kunne potentielt være en betydelig hæmsko for en virksomheds produktivitet og arbejdsgang.

"Det giver jo de her flaskehalse, eller single points of failure, hvor, hvis der er én ting i VPN-konfigurationen eller virksomhedens internetlinje eller lignende, som er ude af drift, af en eller anden grund, eller der er en fejl på den, så er det jo alle medarbejdere, der ikke kan arbejde."

(*Bilag 1*)

Licenser

Overgangen til hjemmekontorer med arbejdsgange, der primært er understøttet af VPN-løsninger, betyder, at der kan opstå mange af disse *single points of failure*, kritiske knudepunkter, der ikke kan omgås, og blot en enkelt brist i kæden kan lede til både spild af arbejdstimer og ressourcer.

Et af de mest bemærkelsesværdige points of failure, der opstod under skiftet til hjemmearbejde, var anvendelsen af VPN-løsninger, rent logistikmæssigt. Langt de fleste større virksomheder

benytter sig af VPN-pakkeløsninger fra tredjepartsforhandlere, såsom for eksempel Cisco med deres udbredte *AnyConnect* VPN-produkt. Essentielt set fungerer disse således, at virksomheden køber et specifikt antal licenser til produktet, som så benyttes af de ansatte, der befinder sig uden for virksomhedens fysiske områder.

"Det er også en typisk udfordring, at man har købt licenser til, at der skal være måske 20% af medarbejderne på via VPN på én gang"

(*Bilag 1*)

VPN-løsningen er tiltænkt som et fleksibelt hjælpeværktøj, der tillader ansatte at fortsætte deres arbejde uden fysisk tilstedeværelse i virksomheden, men den har aldrig været intenderet til at være en erstatning af den fælles arbejdsplads, og mængden af indkøbte licenser afspejler denne tankegang (Bilag 4).

Omstillingen til hjemmearbejde for et markant højere antal ansatte har imidlertid også haft logistiske konsekvenser for såvel VPN-anvendende virksomheder som de VPN-udbydende virksomheder, og specielt hvis serviceudbyderen er en af de mest anvendte, såsom Cisco.

"Vi bruger Ciscos produkt, der hedder AnyConnect… Det er klart, det er jo næsten en branchestandard, kan du sige."

(*Bilag 1*)

Den storstilede omstilling til hjemmearbejdspladser betød imidlertid, at de fleste virksomheder pludselig stod med et underskud af VPN-licenser, som de kunne allokere til deres hjemmearbejdende ansatte. Normalvis ville en supplering af yderligere licenser umiddelbart ikke være en tidskrævende eller ressourcetung proces, men når udbyderen benyttes i så vidtstrakt en størrelsesorden som Cisco, kan den pludselige strøm af licensefterspørgsler fra adskillige kunder resultere i noget ekstra ventetid for både kunder og udbyder.

"Et godt eksempel var, da alle blev sendt hjem, og ingen virksomheder havde købt licenser nok til alle. Så blev Cisco, fordi de også er den klart største udbyder af det her, jo nærmest væltet af alle de kunder, der ville købe ekstralicenser lige nu og her."

(*Bilag 1*)

Ændring af arbejdsgang

Omstillingen til hjemmekontorer har for mange virksomheders vedkommende været en tidskrævende og flerspektret sag, og det har ikke kun været rent teknologiske udfordringer, der har været bemærkelsesværdige under denne proces. Hjemmekontoret, og alle de tekniske og logistiske udfordringer, disse indebærer, har været et wildcard for både de hjemmearbejdende ansatte samt de IT-sikkerhedsansvarlige, der skal sørge for, at alting foregår som det skal. De hjemmearbejdendes forhold er ikke lige så simple at holde styr på, som hvis de befandt sig på kontoret og benyttede sig af virksomhedens lokalnetværk og udstyr. Ligeså kan det isolerende element i omstillingen til hjemmekontorer føre til forstyrrelse af arbejdsgange, samt forvirring i forhold til korrekt, IT-sikkerhedsmæssig adfærd.

"… fordi vi kunne jo se, at folk var sendt hjem, og de sidder i en stresset situation og sådan noget, og så er du bare mere latent til at klikke på noget. Og hvis man sidder derhjemme, er det ikke altid, man lige husker at genstarte maskinen eller lukke maskinen, så får man bare lige klappet ned, og så starter man igen næste morgen, så vi kunne ikke garantere, at vi havde vores opdateringer ude."

(*Bilag 2*)

En af de mere prominente, IT-sikkerhedsrelaterede udfordringer for virksomheder generelt, både før, men især efter omstilling til hjemmekontorer, er beskyttelse af de ansatte imod digitale angreb, såsom phishingforsøg, eller de mere målrettede spear-phishingangreb. Disse angreb har i sinde at udhale adgangsgivende informationer fra ansatte, ved at få dem til at indtaste for eksempel deres loginoplysninger på en hjemmeside og på den måde bringe virksomhedens sikkerhed i fare. Isoleringsfaktoren, i sammenhæng med en stressende ændring af arbejdsforhold, kan potentielt gøre den individuelle ansatte mere sårbar over for denne form for manipulation. Især nøglepersonale, såsom ansatte med dybere adgang til systemer, er særligt udsatte, hvad angår målrettede spear-phishingforsøg.

> *"Hvis vi har at gøre med en systemadministrator, og de skriver på LinkedIn 'jeg er systemadministrator', jamen så har de sgu nok en administrativ adgang. Så spear-phishing, det er mere sandsynligt til denne her gruppe administrative medarbejdere… Så dem skal vi gøre noget ved, dem skal vi adressere."*
>
> (*Bilag 2*)

> *"Så længe de brugte VPN og proxy, så var det ligesom at være på kontoret. Der er mange, der har råbt 'uha, det er farligt her under Corona' og så noget, men hvad er den øgede risiko? Der er ikke nogen, der har kunne fortælle mig det helt specifikt, andet end der er en øget phishingaktivitet…"*
>
> (*Bilag 2*)

Dog har den vidtstrakte, og som regel virksomhedspålagte, anvendelse af IT-sikkerhedsforanstaltninger, primært i form af VPN-løsninger, været effektiv, og den har dermed øget IT-sikkerheden hos de individuelle ansatte på hjemmekontorerne til et acceptabelt niveau. Omstillingen til hjemmekontorer har muligvis været mindre IT-sikkerhedsudfordrende end tidligere ventet, i fald de ansatte er klar over, hvilke sikkerhedsforanstaltninger de er underlagt, og hvilke risici de skal være agtpågivende overfor.

I nogle tilfælde, hvor der er stigende systembelastning på virksomhedens VPN-forbindelse, og irritationsfaktoren over langsomme forbindelse for de ansatte på hjemmekontorerne dermed også stiger, kan det forekomme, at ansatte forsøger at tage sagerne i egen hånd for at forbedre arbejdsforholdene. Kombineret med hjemmekontorets isolerende natur og mangel på opsyn fra virksomhedens IT-afdeling kan dette føre til ikkegennemtænkte handlinger, der potentielt kan bringe virksomhedens IT-sikkerhed i fare, specielt fordi disse handlinger kan være svære at detektere fra IT-afdelings side.

"Dem, som der er lidt bekymrede eller bange, eller ikke helt forstår det, de skal nok følge alle reglerne, men dem, som tænker 'jeg kan alt det med IT selv, jeg skal nok finde en bedre firewall selv', det er typisk der, det går galt. Nogle gange kan de sikkert godt, og det opdager vi så ikke, og det er sikkert fint nok, og andre gange får de måske truffet nogle valg, der ikke var helt så hensigtsmæssige."

(*Bilag 1*)

"Men styrken i VPN, der er det, at det er virksomheden der sætter en policy… Du kan ikke komme udenom det, og der er ikke nogen andre, der kan dumme sig og lave et eller andet, så det ikke er stærkt nok."

(*Bilag 1*)

Når majoriteten af de ansatte befinder sig på kontoret og benytter sig af virksomhedsverificeret hardware, er risikoen for, at en ansat kommer til at bringe virksomhedens IT-sikkerhed i fare, drastisk reduceret. Derfor er udfordringer som disse vigtige at imødekomme for at undgå utilsigtede fejltagelser, men implementeringen af VPN-løsninger til hjemmearbejdet synes at være en effektiv løsning til de fleste af de problemstillinger.

Interaktion mellem ansatte

Et andet aspekt af omstillingens konsekvenser er, hvordan kontakten mellem de ansatte og virksomheden foregår, samt hvordan den interne kontakt imellem individuelle ansatte i de forskellige afdelinger af virksomhederne foregår. Videokonferenceplatforme er blevet normen for de hjemmearbejdende, som ikke nødvendigvis har været nødt til, eller haft behov for, at benytte disse før hjemsendelsen.

> *"Der er selvfølgelig sket en kæmpe forandring. Specielt med Teams. Jeg tror faktisk ikke, jeg har brugt Teams, før vi fik det her Corona. Så det er en ny måde for mig at kommunikere og arbejde på."*
>
> (*Bilag 7*)

Skiftet til at benytte udelukkende videokonferenceplatforme, såsom Microsoft Teams, har medført en forandring i, hvordan dynamikken mellem ansatte foregår, eller måske snarere en alternativ benyttelse af de nye omgivelser til at simulere mere vante omgivelser.

> *"Nogle gange lægger vi faktisk ikke på, når vi holder møder. Så kan mødet stå tændt hele dagen. Det er lidt ligesom i et kontormiljø, du ved, hvor man lige kan råbe efter en kollega og spørge, om vedkommende ikke lige kan hjælpe med et eller andet."*
>
> (*Bilag 7*)

Simuleringen af denne form for velkendt kontormiljø, med kollegaer indenfor rækkevidde til at sparre med, kan endvidere potentielt også være en mitigerende faktor, hvad angår at beskytte sig imod for eksempel phishingforsøg, idet det er nemmere at trække på de andre medarbejdere, der kan hjælpe med at identificere en mistænkelig interaktion. Phishingangreb er som oftest rettet

mod enkelte ansatte eller grupperinger af ansatte, og angrebene er især farlige, når disse ansatte er isolerede og ikke i momentet kan trække på andre ressourcer. Men den digitale genskabelse af kontoret kunne være en effektiv måde, hvorpå de ansatte kan arbejde sammen om at vedligeholde IT-sikkerheden.

> *"… det sker en gang imellem, hvor vi får en mail, som vi ikke er helt sikre på om er legit eller ej. Så spørger vi lige rundt, om der er nogen, der ved noget om noget, når ham der Troels, eller hvad han nu kan hedde, vil have alle mine informationer til et eller andet."*
>
> (*Bilag 7*)

Anvendelsen af videokonferenceplatforme, til på denne måde at simulere en hel arbejdsdag, har både positive bivirkninger, som de ovenstående, men potentielt også negative bivirkninger såsom båndbreddebrugen til videostreaming. Normalvis ville en sådan forbindelse køre igennem virksomhedens VPN-forbindelse, og et møde, der kører en hel dag, kræver en masse ressourcer, specielt hvis der over hele perioden også deles livevideo fra flere parter.

Nye medarbejdere

En yderligere vinkel på, hvordan omstillingen har haft en effekt på den normale arbejdsgang, er tilføjelsen af nye ansatte under omstillingsperioden. Manglen på fysiske interaktioner, og muligheden for at integrere nyligt ansatte medarbejdere i en fastsat og stabil arbejdsrutine, præsenterer også en udfordring.

> *"Det har også været svært i en rekrutteringsfase at on-boarde. Jeg fik jo 4 nye medarbejdere, men vi var sendt hjem i foråret. Hvordan on-boarder du en ny medarbejder, altså hvordan får du en ny medarbejder ind i virksomheden, hvis de skal sidde derhjemme? Det er bare sådan, at jeg mødte dem inde på*

kontoret og udleverede deres PC, og så gik vi hjem, og så sås vi 2 måneder efter."

(Bilag 2)

Hvilke behov søger VPN-teknologien at løse ved omstillingen til hjemmekontor?

Den primære grund til, at virksomheder vælger at implementere en VPN-forbindelsen til de hjemmearbejdendes arbejdscomputere, er at danne et sikkerhedsnet for virksomhedens data. VPN-teknologien tilbyder et sikkerhedsnet af forsvarsmekanismer, som datahåndteringen ville stå foruden, når en virksomheds ansatte arbejder hjemmefra.

"(…) vi har nogle forsvarsmekanismer, alt fra firewalls til webproxyer, der skal søge efter malware, DNS inspection og alle mulige beskyttelser, der er sat op i virksomheden. Så vil vi jo godt have, at selvom medarbejderne sidder derhjemme, så gør de også brug af det samme niveau af beskyttelser, og det sikrer vi jo med en VPN-forbindelse. Fordi så kører det hele jo igennem der."

(*Bilag 1*)

Derudover opretter VPN-teknologien en krypteret linje imellem de hjemmearbejdendes computere og virksomhedens server. På denne måde kan de ansatte kommunikere og bearbejde virksomhedsdata, uden at de aktivt skal tage stilling til sikkerhedsniveauet ved denne datahåndtering. VPN-forbindelsen fører internettrafikken ud igennem virksomhedens internetforbindelse, i stedet for via de hjemmearbejdendes private internetforbindelse. Dette er et vitalt led i sikringen af virksomhedsdatabearbejdelse, eftersom de hjemmearbejdendes private internetforbindelse ikke er opsat efter virksomhedens retningslinjer, og derved heller ikke overholder de potentielle politikker, virksomhedens data følger (Bilag 1). De hjemmearbejdendes private internetforbindelse kan desuden være opsat, før de ansatte eventuelt er blevet introduceret til sikker, digital adfærd, hvorfor simple, private internetforbindelser kan have flere bagdøre og huller i sikkerheden.

Vores informanter har givet udtryk for, at der er blevet implementeret en VPN-forbindelse imellem virksomheden og deres hjemmekontorer, hvorfor virksomheden har fokuseret på at introducere de ansatte til, hvordan denne virker, snarere end at undervise de ansatte i sikker, digital adfærd. Dette medfører en manglende forståelse for, hvad de ansatte skal være særligt opmærksomme på, når de arbejder hjemmefra, og endvidere en manglende forståelse for den sikkerhedsmæssige årsag til, at virksomheden anvender VPN-teknologi (Bilag 3). Dette kan gå hen at blive problematisk, hvis scenariet om en mistet VPN-forbindelse skulle opstå, for eksempel hvis licensaftalen ophører, eller hvis arbejdscomputeren går i stykker, så den hjemmearbejdende er nødsaget til at håndtere virksomhedsdata fra sin private computer. Her er den ansatte så ikke undervist i, hvordan sikkerhedsprotokollen for den anvendte VPN-løsning ser ud, og overholder derfor heller ikke denne. En af de hjemmearbejdende informanter gav udtryk for, at virksomheden formulerede nogle retningslinjer til sikker adfærd:

> *"I forbindelse med at jeg startede med at arbejde hjemmefra, fik jeg en "flyer", hvori forskellige regler i forbindelse med IT-sikkerhed blev udpenslet. Herunder, at man kun måtte anvende ens arbejdscomputer på ens eget netværk. (…) Jeg følger de forskrifter, som jeg kan huske, der kom fra den føromtalte flyer. Jeg har, efter en hurtig søgning på intranettet, dog ikke kunne finde den."*
>
> (*Bilag 6*)

Ud fra dette citat giver den hjemmearbejdende informant udtryk for, at introduktion til sikker digital adfærd er sket i et sparsomt omfang, som efterfølgende kan være vanskeligt at finde igen. Hvis scenariet med en svigtende VPN-forbindelse skulle finde sted, vil den hjemmearbejdende være afhængig af hukommelsen omkring den uddelte flyer, og hvad der står foreskrevet i denne, i forhold til at tilgå virksomhedens data.

En anden informant italesatte ligeledes, hvordan vedkommende er blevet undervist i IT-sikkerhedsansvarlig adfærd af sin virksomhed. Dette har ikke været i forbindelse med omstilling til hjemmekontor, men snarere med fokus på generel, sikker adfærd, hvor virksomheden med mellemrum udsender videoer med tilhørende testspørgsmål, som de ansatte skal svare på. Problemet ved disse IT-sikkerhedsvideoer bliver dog beskrevet som, at indholdet er basalt og niveauet er for lavt, hvorfor det faglige udbytte ikke synes at være tilstrækkeligt. Selvom virksomheden investerer opmærksomhed i IT-sikkerhed og digital adfærd, virker den information, der bliver tilsendt, ikke tilstrækkelig. Derfor, da vi adspurgte den hjemmearbejdende medarbejder, om de ansatte nogensinde bliver undervist i IT-sikkerhed, udtrykker vedkommende en tvivl omkring egne IT-sikkerhedskompetencer, ved afsluttende at udtrykke:

"både ja og nej, da vi bliver undervist på det her niveau"

(*Bilag 7*)

Hvad angår de hjemmearbejdendes egne initiativer til at sikre virksomhedens data, gives der i nogle tilfælde udtryk for modsatvirkende handlinger, der uforsætligt bringer virksomhedens data i fare. Dette italesættes blandt andet ved at opbevare data på private drev, hvilket går udenom virksomhedens sikkerhedsprotokoller (Bilag 5).

Ud fra de interviews, vi har foretaget til dette projekt, italesætter de hjemmearbejdende informanter enkelte frustrationer over sikkerheds-check-points og langsom hastighed på VPN-forbindelsen. Dette kan i nogle tilfælde forstyrre de hjemmearbejdendes arbejdsgang og derved forsinke udbyttet af arbejdsopgaverne (Bilag 3 & bilag 7). Hvis dette når en grad, hvor de ansatte ikke kan udføre deres arbejde, kan virksomheden risikere, at enkelte hjemmearbejdende ansatte ændrer på sikkerhedsopsætningen på deres VPN-forbindelse, og derved gør deres computer sårbar over for angreb.

"Nogle af de ting, man godt kunne se rundtomkring, er, at folk synes, at det går for langsomt via VPN, firewall er begrænsende og så videre, og så slår nogle af de ting fra. Det går måske imod nogle sikkerhedsregler, men hvis det kan lade sig gøre rent teknisk, så er der måske nogle, der kan finde på det alligevel. Og hvis det sker, så bringer man IT-sikkerheden i virksomheden i fare."

(*Bilag 1*)

Som citatet forklarer, er det ikke garanteret, at alle VPN-udbydere tillader at ændre i teknologiens opsætning uden at have administrative rettigheder, hvilket de hjemmearbejdende ansatte som udgangspunkt ikke har. Men skulle dette alligevel kunne lade sig gøre for nogle medarbejdere, vil dette modstride virksomhedens sikkerhedspolitik og derved potentielt medføre, at de kan udsættes for digital uret.

Ud fra den empiri, vi har indsamlet fra hjemmearbejdende ansatte, giver deres udsagn udtryk for, at deres ansvar for IT-sikker adfærd og datahåndtering skal tydeliggøres af virksomhederne i form af retningslinjer og undervisning i konsekvenserne ved mangel på IT-sikkerhed. For at opnå en alvorskonsensus skal denne information om sikker, digital adfærd desuden formidles i et format, der signalerer seriøsitet. Der nævnes pjecer og korte videoer med dertilhørende tests som eksempler på, hvad virksomheder har anvendt af mislykkede kommunikationskanaler for at informere de ansatte om IT-sikkerhed. Derudover udtrykkes der et tilgængelighedsproblem for de ansatte, hvilket kommer til udtryk i form af frustration over, at en langsom VPN-forbindelse har konsekvenser for arbejdsgangen og udbyttet heraf (Bilag 6 & bilag 7). Dog udtrykkes der ligeledes et potentiale for IT-sikkerhedsmæssige sårbarheder for virksomhedens data, hvis de ansatte skulle have muligheden for, og skulle kunne finde på at deaktivere enkelte sikkerhedsopsætninger i VPN-forbindelsen, så de derved kan bringe virksomheden i fare for digitale angreb.

Diskussion

Der skal ikke herske tvivl om, at VPN-løsninger har været en uvurderlig teknologi, når det kommer til omstillingen til hjemmekontorer. Alligevel kan det være relevant at analysere og diskutere de ting, som VPN-teknologien måske ikke gør så godt. Et af hovedformålene med VPN-teknologien er at kunne tilgå virksomhedens data fra eksempelvis en hjemmearbejdsplads. Det kan der være flere grunde til, men ofte handler det om, at medarbejderen har brug for at arbejde med data eller information, som er personfølsom, og derfor kræver visse sikkerhedsmæssige tiltag, så det kan sikres, at de ikke ender i de forkerte hænder, eller bliver misbrugt. VPN-teknologien er med sine mange sikkerhedsmekanismer den førende teknologi inden for denne type af omgang med data.

Dog er det ikke alt arbejde fra et hjemmekontor, VPN-teknologien nødvendigvis er den bedste metode at sikre arbejdet med. De interviews, der er blevet udført i forbindelse med dette projekt, har vist, at mere og mere datatrafik fra hjemmekontorerne bliver dirigeret udenom virksomhedernes VPN-forbindelser. En årsag skal findes i, at VPN-kapaciteten ikke har været stor nok til at håndtere den nye, større mængde trafik fra det nye, store antal hjemmearbejdende. En anden årsag skal findes i, at antallet af brugslicenser til virksomhedernes VPN-forbindelser ikke var tilstrækkeligt. En løsning på kapacitetsproblemet skulle vise sig at være en omdirigering af datatrafik, der enten var tiltro til, eller som var af ikke-kritisk karakter. Med denne split-tunnelling-løsning, eller trafikomdirigering, blev mængden af trafik tilpasset VPN-kapaciteten, så kun den kritiske datatrafik blev sendt via VPN-forbindelsen, hvorimod resten af datatrafikken blev sendt udenom. En løsning på licensproblemet var blot at købe flere licenser, så de ansatte kunne koble op på deres VPN-forbindelse og arbejde, som det nu en gang var dem tiltænkt. Dette stiller så spørgsmålet: Hvilken VPN-kapacitet har virksomheden egentligt brug for?

Databeskyttelse og cloud-baserede tjenester

Mange moderne og større virksomheder bruger programmer og digitale tjenester, som deres medarbejdere også bruger i deres private liv. Tjenester som Outlook Mail, Skype, Microsoft Office og Microsoft Teams er eksempler på tjenester, som mange virksomheder bruger, og som medarbejderne også bruger privat. Dette har flere fordele. Eksempelvis gør det faktum, at brugerne også bruger tjenesterne privat, det nemmere at arbejde hjemmefra, fordi de kender de

funktionelle mekanismer i programmerne fra privat brug. Ydermere gør det det også lettere at lære nye medarbejdere op, fordi de sandsynligvis vil kende tjenesterne fra andre jobs eller privat brug. Grunden til, at disse løsninger er så udbredte, er blandt andet, at de er billige at købe licenser til og lave aftaler om. Derudover er tjenesterne også cloud-baserede, hvilket gør dem ekstremt bekvemme at bruge på farten eller hjemmefra. Alle disse kvaliteter er med til at gøre brugen af disse tjenester attraktive. De kan øge tilgængeligheden for hjemmearbejde, fordi de kun kræver, at medarbejderne har et hjemmenetværk, de er billige, og mange kender dem i forvejen. Derfor kan det være svært for en virksomhed at vurdere, hvornår man kan stole på, at ens data er ordentligt beskyttet hos en tjeneste, og beskyttet nok til, at man kan benytte sig af den. Datatilsynet i Danmark har ikke lavet nogen overordnede vurderinger af for eksempelvis Googles eller Microsofts tjenester, og det er derfor op til den enkelte virksomhed, selv at undersøge og vurdere, om en tjeneste er sikker nok eller ej. Den proces, det kræver at finde ud af dette, er meget tidskrævende og omkostningstung. Særligt offentlige institutioner og virksomheder lider under dette. Chief Information Officer i Ballerup kommune udtaler til Ingeniøren:

> *"Jeg synes virkelig, de enkelte kommuner er ladt i stikken. Hvis de ikke alle sammen er knivskarpe på alt i forhold til GDPR og databeskyttelse – skarpere end mange advokathuse – så kommer de til at gøre noget forkert. Og det er her, jeg synes, kæden hopper af. Der er brug for, at der er nogen, der træder frem og siger noget" – Jens Kjellerup 2021*
>
> (Fribo, 2021, 4)

Denne udtalelse drejer sig om EU's erklæring om, at USA er et usikkert tredjeland, hvilket betyder, at man ikke må overføre persondata til landet. Dette er et eksempel på, hvor mange forskellige ting, der spiller en rolle i, om noget kan vurderes sikkert eller ej, og dette har gjort, at mange offentlige instanser og virksomheder er i gang med at omlægge deres arbejdsgang.

Et stort problem, som forbinder sig til brugen af cloud-baserede løsninger i en professionel forbindelse, er, at de udfylder et behov, hvor der på nuværende tidspunkt ikke kan findes leverandører af lignede tjenester, som kan vurderes som værende sikre og samtidig udfylde dette

behov. Erklæringen om, at der ikke længere må sendes personfølsomme data til USA, har fået giganten Microsoft til at omlægge deres infrastruktur således, at de fremover kan garantere, at den personfølsomme data bliver i Europa. Det er endnu ikke sikkert, hvad fremtiden bringer i forhold til databeskyttelse, men Microsoft lader til at have taget et skridt i den rigtige retning med deres nye initiativ, og så kan man kun spå om, hvorvidt andre leverandører vil følge trop.

VPN og HTTPS

Når man taler om databeskyttelse hos cloud-baserede tjenester, er det relevant at nævne HTTPS. HTTPS står for *Hypertext Transfer Protocol Secure*, og er den sikkerhedsmekanisme, mange cloud-baserede IT-tjenester benytter til at beskytte data på nettet. HTTPS benytter af sig af samme princip om kryptering af data som VPN-teknologien. Kort fortalt beskytter protokollen altså data, således at de ikke kan overvåges, ændres eller stjæles, når man bruger sin internet-browser. Alligevel er der problemer, som forbinder sig til dette paradigme. Tjenester og applikationer taler mere med internettet end de fleste brugere ved, og det er svært at finde ud af, om denne kommunikation er sikker eller ej. HTTPS kan kun beskytte dine data gennem din internet-browser, og altså ikke nødvendigvis den kommunikation, tjenester på en computer har med internettet. Ydermere kan HTTPS også være sårbar overfor visse typer af angreb. Særligt angreb, hvor hackeren får det til at se ud, som om vedkommende er *root*-certificeret. Denne type angreb gør, at hackeren får mange muligheder, eftersom *root*-certifikation er det dybeste niveau, der findes i hjemmesiders brugerhierarki.

VPN-teknologiens mange sikkerhedsmekanismer gør det ekstremt svært at overvåge eller stjæle information, når forbindelsen er åben. Dette tillader, at en bruger kan forbinde til en virksomheds netværk uden frygt for, at forbindelsen er kompromitteret. Når brugeren er på virksomhedens netværk, vil der typisk være mange sikkerhedstiltag, så som firewall-konfigurationer, site-blockers, valideringer og timeout-regler. Der, hvor VPN-teknologien på hjemmekontorer måske er særligt udsat, er i de tilfælde, hvor man på virksomhedens netværk ikke kan se, hvilken fysisk person, der bruger forbindelsen, men blot ved, hvem brugeren *burde* være. Har brugeren eksempelvis forladt sit hjemmekontor uden at låse computeren eller lukke VPN-forbindelsen til virksomheden, kan enhver, som skaffer sig adgang til hjemmekontoret, bruge forbindelsen. Dette scenarie er

usandsynligt, men alligevel værd at have in mente, da VPN-løsninger nu har indbyggede timeout-regler, der sikrer, at forbindelsen afbrydes, hvis ikke den bruges aktivt. En anden udfordring kan være, at en medarbejders computer kan være inficeret med spyware, som tillader hackere eller digital-kriminelle at overvåge skærmen. Dog er denne trussel også usandsynlig, og den kan omgås, i fald at medarbejderen ikke falder for phishing-mail, eller hvis medarbejderens computer at styret af virksomheden og ikke kan benyttes privat.

Hvad angår at sammenligne VPN og HTTPS kan det nævnes, at begge teknologier benytter kryptering til databeskyttelse. HTTPS krypterer den data, som sendes mellem internet-browseren og IT-tjenesten, hvorimod VPN-teknologien krypterer alle data, såfremt der er forbundet til dem. Måden de to løsninger krypterer på er også forskellig. VPN-teknologien bruger en række værktøjer, så som *encapsulation* og *tunnelling*, hvorimod HTTPS benytter sig af en nøgle, som dannes i korte perioder (*sessions*) og derefter atter forsvinder. Disse nøgler er svære at finde noget information om, og det er derfor også svært at vide, hvor sikre de er.

Det kan være svært at spå om fremtiden for IT-organisationer. Cloud-baserede IT-tjenester, som benytter HTTPS, er i og for sig sikre, men alligevel er der nogle typer angreb, tjenesterne er sårbare overfor. Det særligt tiltrækkende ved Cloud-baserede IT-tjenester er deres tilgængelighed, da de er både billige og skalérbare. Langt dyrere er det, hvis en organisation eller virksomhed skal have udviklet lignende tjenester, som brugere kun kan tilgå ved at etablere en VPN-forbindelse til virksomhedens netværk. Dette fjerner også noget tilgængelighed, fordi der er flere led, hvori forbindelsen kan fejle. Til gengæld kan man ved brug af VPN-teknologien, apparater styret af organisationen og IT-sikkerhedsuddannelse af medarbejdere, garantere et meget højt niveau af sikkerhed. Mange virksomheder er i gang med at finde en balance mellem HTTPS og VPN, men det er en lang proces, eftersom der er rigtig mange parametre at tage stilling til. Ultimativt må en balance mellem, hvilke tjenester, der er sikre at bruge til hvad, hvor specifik data, der skal behandles, og hvilken grad af styring af IT-apparater, virksomheden skal have, være den mest økonomiske, passende og sikre løsning for fremtidens IT-organisationer.

Adfærdsdesign

Hvad angår omstilling til hjemmekontorer bidrager VPN-teknologien til IT-sikkerheden og tilbyder derved en løsning på det behov, som hjemmearbejdende har for sikker, digital adfærd. Dog kan et andet aspekt omkring øget IT-sikkerhedsopmærksomhed på hjemmekontoret, såvel som på virksomhedens kontor, øges ved at prioritere at undervise virksomhedens ansatte i IT-sikkerhed. Ved at investere i kurser og undervisning om IT-sikkerhed og digital adfærd, der giver et reelt fagligt udbytte, i modsætning til interne mails om phishing, agtpågivenhed eller korte videoer med dertilhørende test (Bilag 7 & Bilag 5), kan de ansatte potentielt lære at inkorporere en korrekt sikkerhedsmæssig adfærd. Det kan blive et spørgsmål om at designe en ønsket adfærd til de ansatte medarbejdere, så de udvikler en forståelse for alvoren omkring digital uret og danner et sikkerhedsniveau herefter. Hvis der opnås en udviklet IT-sikkerhedsadfærd blandt de ansatte, vil denne kunne gavne brugen af VPN-teknologien, og frygten for bagdøre og sikkerhedshuller i VPN-forbindelsen kan derved formindskes. Derudover kan undervisning i alvoren ved sikker adfærd potentielt give de ansatte en forståelse for, at de skal holde både deres private computere og arbejdscomputere rene for software og andet materiale, der potentielt kan indeholde virus eller anden spyware.

Dog skal dette IT-sikre adfærdsdesign også tage højde for fokus på en intuitiv adfærd, således at tilgængelighedsaspektet af IT-sikkerheden bibeholdes. Datatilgængelighed er oftest et fokus, der lægges på en IT-sikkerhedsteknologi, hvor anvendelse af teknologien blandt andet ikke skal være forstyrrende for de ansattes arbejdsgang, for eksempel ved mange sikkerheds-check-points. Dog kan der argumenteres for, at et adfærdsdesign med fordel kan tage højde for tilgængelighedsaspektet, netop for at lægge vægt på intuitiv inkorporering af sikker, digital adfærd.

Konklusion

Som direkte svar på projektets problemformulering: " Hvilke udfordringer har der været med data-tilgængelighed i forbindelse med hjemmekontorsomstillingen, og hvilken indflydelse har VPN-teknologien haft herpå?", har der været flere udfordringer med datatilgængelighed i forbindelse med omstillingen til hjemmekontorer. Der er i omstillingen kommet flere muligheder for at miste forbindelsen til virksomhedens netværk, fordi der er flere led til opkoblingen end tidligere. Inden omstillingen, hvor de ansatte hovedsageligt befandt sig fysisk i virksomheden, handlede det kun om, hvorvidt virksomheden havde internetforbindelse, og ifald de ikke havde, ville der i mange tilfælde være arbejdsopgaver, som ikke krævede internet, idet der allerede var forbindelse til virksomhedens netværk. Efter omstillingen kan der nu også være problemer hos medarbejderne, hvis de ikke har forbindelse, og ligeledes kan virksomheden og internetudbyderen også forsat have problemer. Ydermere forårsagede den pludselige hjemsendelse af størstedelen af den danske arbejdskraft ligeledes store flaskehalsproblemer, fordi så massive mængder af brugere forsøgte at forbinde på samme tid. Dette var hverken virksomhederne eller VPN-udbyderne klar til, da det krævede flere licenser, end der var til rådighed, og en anden måde at benytte VPN-teknologien på. I forhold til, hvordan VPN-teknologien har haft indflydelse på omstillingen til hjemmekontorer, kan det nævnes, at VPN-teknologien har vist sig at være en stærk allieret. Den har i mange virksomheders tilfælde været ene om at sikre muligheden for at arbejde hjemmefra. En årsag til dette er blandt andet den krypteret forbindelse, som VPN-teknologien opsætter imellem arbejdsstederne via *tunnelling*. VPN-teknologiens IT-sikkerhedsmekanismer har givet medarbejderne mulighed for at arbejde hjemmefra som normalt, fordi truslerne mod teknologien er få, og der er langt imellem. Dog bør det også nævnes, at VPN-teknologien også var med til at skabe problemer med tilgængelighed indledningsvist i omstillingen. Forbindelseshastigheden til virksomhedens data kan være langsom, hvilket kan forstyrre de ansattes arbejdsgang, deres workflow, og dermed også den tilgængelighed, de har til virksomhedens data.

Perspektivering

Med henblik på at fortsætte dette projekt i et designorienteret perspektiv kan en videreudvikling være at se på, hvordan en VPN-løsning kan designes til små virksomheder. Herved perspektiveres

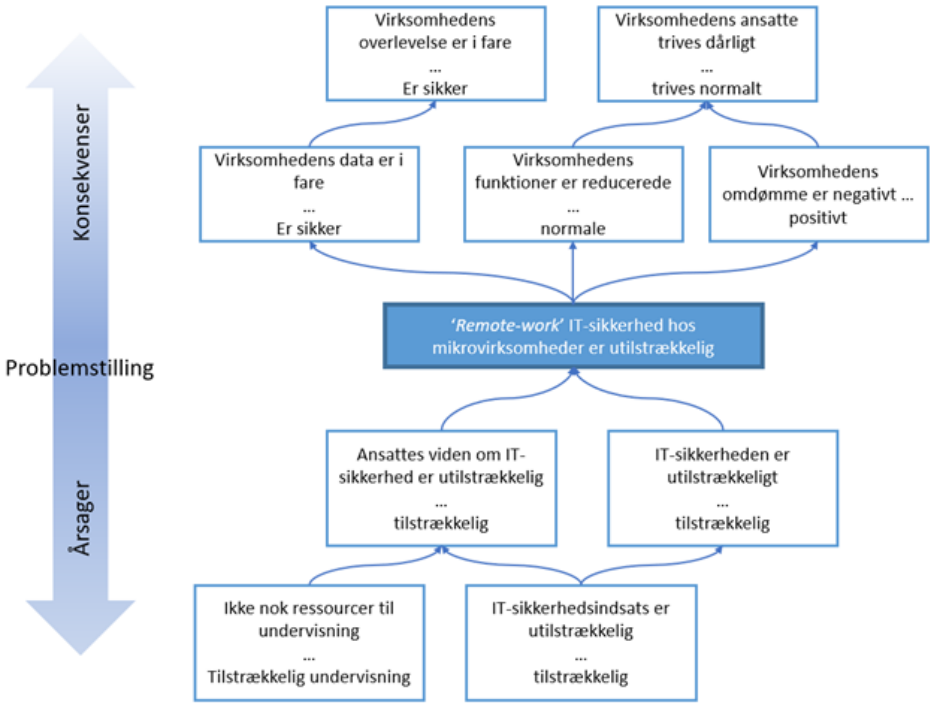
der til tidligere projekter, hvor vi i gruppen har arbejdet med IT-sikkerhed i mikro-virksomheder. En videreudvikling af projektet kan undersøge en mulig designløsning ud fra små, danske virksomheders behov for IT-sikkerhed, og dermed bruge resultaterne fra dette projekt som springbræt. Derved kunne en fremtidig forskning herom undersøge, hvilke problemstillinger små virksomheder møder, hvad angår IT-sikkerhed, og endvidere, hvilke løsninger en VPN-forbindelse kan tilbyde beskyttelsen af små virksomheders data.

Hvordan kan en sikker '*remote working*'-løsning designes for mindre virksomheder?

Gruppens tidligere undersøgelser af IT-sikkerhedsforholdene hos mikrovirksomheder (5 eller færre ansatte) kunne konkludere, at IT-sikkerheden ofte blev nedprioriteret, hvad angik uddelegeringen af arbejdsroller. En af de årsager, vi fandt, var, at der sjældent var én decideret IT-sikkerhedsspecialist, og at IT-sikkerhedsansvaret var en fælles rolle, som alle påtog sig passivt. Dette kan vise sig at være en problematisk tilgang, idet alle ansatte i disse virksomheder allerede gaber over adskillige roller, og der sjældent er udarbejdet en decideret IT-sikkerhedspolitik i virksomheden (Nielsen, Petersen, Stilling, Støvring, 2019, 62).

Hvad angår at at skulle designe en '*remote working*'-løsning for virksomheder i denne størrelsesorden, er aspekter som antallet af den enkelte ansattes roller i virksomheden relevant, samt hvordan disse roller formgiver og understøttes af den adfærd og de vaner, arbejdsgangen genererer. Heri kan der med fordel inddrages adfærdsdesign som en af de primære drivkræfter i designprocessen; et design, der lægger vægt på de ansattes, ofte multifacetterede arbejdsbyrder, og hvordan disse bedst kan understøttes af en IT-sikkerhedsopfyldende designløsning. Adfærdsdesign som designmetode forsøger at imødekomme, hvordan den ønskede adfærd kan defineres ud fra selve designets anvendelse, samt at designløsningen i sig selv baseres på viden om menneskelig adfærd (Pries-Heje, 2018). Baseret på den viden, dette projekt har indsamlet om omstillingen til hjemmekontorer hos primært større virksomheder, og i kombination med viden om arbejdsroller i mikrovirksomheder, kan inddragelsen af adfærdsdesign være en effektiv måde, hvorpå der kan designes en nedskaleret IT-sikkerhedsløsning til mindre virksomheder.

Alternativt kan den indsamlede viden benyttes på en mere systematisk og analytisk måde ved at udvikle en designløsning, der har fokus på en primær problemstilling, hvorfra de forskellige aspekter af '*remote-working* '-omstændigheder udspringer, samt deres iboende konsekvenser. Problemkortlægningsmetoden, *Colored Cognitive Mapping for Design Science Research* (CCM4DSR), beskriver en måde, hvorpå der kan genereres et visuelt overblik over, hvilke problemstillinger en designløsning skal håndtere. Disse problemstillinger kan herefter vendes til en forklaring på, hvordan problemstillingerne kan løses, og hvilke konsekvenser disse designløsninger resulterer i (Pries-Heje, 2018).



Figur 6: Eksempel på et CCM4DSR-problemkortlægning over 'remote working'-problemstillingen.

Grundlaget for de forskellige tilgange til at udvikle en designløsning er, at der placeres et fokus på, hvorfor problemstillingen er et problem, samt hvilke aspekter, der spiller ind i, hvordan problemets konsekvenser kan ændres, og hvordan disse ændringer udfolder sig, når en designløsning skal udvikles.

Litteratur

Bøger

Kvale, S. & Brinkmann, S. (2015). *Interview: Det kvalitative forskningsinterview som håndværk*. (3. udg.). København, Danmark: Hans Reitzels Forlag.

Pfleeger, C., Pfleeger, S., & Margulies, J. (2015) *Security in Computing* (5. Udg) Prentice Hall

Stallings, W. & Brown, L. (2018) *Computer security. Principles and practice* (4. Udg) Harlow, United Kingdom: Pearson

Rogers, E. M. (2003). *Diffusion of innovations*. 5th ed. New York: Free Press.

Scott, C., Wolfe, P. & Erwin, M. (1998) *Virtual Private Networks*. (1. Udg) Sebastopol, CA: O'Reilly

Sismondo, S. 2010. *An introduction to Science and Technology Studies*. Oxford: Blackwell.

Tripathy, B.K. Anuradha, J. (2018) *Internet of things (IoT): technologies, applications, challenges and solutions.* CRC Press by Taylor & Francis Group, LLC.

Rapporter Og publikationer

Flyvbjerg, B. (2006). *Five Misunderstandings About Case-Study Research*. Sage publications. pp. 219-242

Fribo, A. (2021) *Myndigheder famler i blinde efter EU's cloud-fatwa*. Ingeniøren 21. udgivelse. 28. Maj 2021. 1. Sektion Side 4-5.

Jørgensen, Niels (2018) *Teknologiers indre mekanismer og processer. Eksemplificeret ved digital signatur*. Undervisningsmateriale til kurset Teknologiske Systemer og Artefakter (TSA), 1. semester, p˚a RUCs humanistisk-teknologiske bacheloruddannelse.

Larsson, S., Svensson, M., de Kaminski, M., Rönkkö, K., & Olsson, J. A. (2012). *Law, norms, piracy and online anonymity: An international journal*. I *Journal of Research in Interactive Marketing*, 6(4), 260-280. doi:http://dx.doi.org.ep.fjernadgang.kb.dk/10.1108/17505931211282391

Nielsen, A., Petersen, J., Stilling M., Støvring, S. (2019). "*IT-sikkerhed i danske SMV-er*" Roskilde Universitet, 3. semester. Humanistisk Teknologisk Bachelor.

Pries-Heje, J (2018) "Design & Konstruktion" Version 1.0. Undervisningsmateriale på den Humanistisk-teknologiske bachelor, Roskilde Universitet, 1. semester. 6. september 2018.

Sommer, M., J & Schraube, E (2018) "Subjektivitet, teknologi og samfund" Undervisningsmateriale på den Humanistisk-teknologiske bachelor, Roskilde Universitet, 1. semester.

Websites

Arildsen, V. (2 december 2020) *På hjemmekontoret er du din egen IT-medarbejder – og det stresser*. Lokaliseret d. 10. april 2021 på: https://www.itu.dk/om-itu/presse/nyheder/2020/paa-hjemmekontoret-er-du-din-egen-it-medarbejder-og-det-stresser

ASCD (15. December 2020) *Assessment on the status of cybersecurity in Denmark*. Lokaliseret d. 5. april 2021 på: https://ascd.dk/results/report.pdf

Cisco1 (u.d.) *What is computer networking?*. Lokaliseret d. 14. maj 2021 på: https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-computer-networking.html#~types-of-networks

Cisco2 (u.d.) *Networking basics: What you need to know*. Lokaliseret d. 14 maj 2021 på: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/networking-basics.html

Cisco3 (u.d.) *How does a switch work?*. Lokaliseret d. 14 maj 2021 på: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/network-switch-how.html

Danmarks Statistik (2021) *Danske hjem bliver mere intelligente.* Lokaliseret d. 22. Maj 2021 på: https://www.dst.dk/da/Statistik/nyt/NytHtml?cid=41576

DanskHR (7. maj 2020) *Ny undersøgelse: Cyberangreb på virksomheder går ud over medarbejdernes privatliv*. Lokaliseret d. 10. april 2021 på: https://danskhr.dk/insights/rapporter/ny-undersoegelse-cyberangreb-paa-virksomheder-gaar-ud-over-medarbejdernes-privatliv/

F5 (11. november 2020) 2020 phishing and fraud report. Phishing during a pandemic. Lokaliseret d. 9. april 2021 på: https://www.f5.com/labs/articles/threat-intelligence/2020-phishing-and-fraud-report

Hogg, S. (2019). *How to prevent IPv6 VPN breakout: Without properly configured remote-access VPNs, IPv6 traffic from remote devices can escape corporate security controls*. Network World (Online), Retrieved from https://www-proquest-com.ep.fjernadgang.kb.dk/trade-journals/how-prevent-ipv6-vpn-breakout/docview/2305962424/se-2?accountid=13607

Ingham, L. (18. februar 2020) Cybersecurity is still an afterthought for two thirds of businesses: EY. Lokaliseret d. 26 maj 2021 på: https://www.verdict.co.uk/cybersecurity-afterthought-ey/

Jeffery, E. (19. juni 2020). *VPN Split-Tunneling – To Enable or Not To Enable*. Hentet fra InfoSecurity Magazine: https://www.infosecurity-magazine.com/opinions/vpn-split-tunneling/

Kaspersky (2020) *Taking care of corporate security and employee privacy*. Lokaliseret d. 10. april 2021 på: https://media.kasperskydaily.com/wp-content/uploads/sites/92/2020/04/20043942/Kaspersky-2020_Report_Human_angle_FINAL.pdf

Kehlet, K. (7. december 2020) *Glansbilledet af hjemmearbejde krakelerer – flere bliver ensomme og depressive*. Lokaliseret d. 15. april 2021 på: https://www.berlingske.dk/arbejdsliv/glansbilledet-af-hjemmearbejde-krakelerer-flere-bliver-ensomme-og

Madsen, Allan (2009): case-studie i Den Store Danske, Gyldendal. Lokaliseret d. 19. maj 2021 på: https://denstoredanske.lex.dk/case-studie

Microsoft (19. august 2020) *New data from Microsoft shows how the pandemic is accelerating the digital transformation of cyber-security*. Lokaliseret 9. april 2021 på: https://www.microsoft.com/security/blog/2020/08/19/microsoft-shows-pandemic-accelerating-transformation-cyber-security/

NetworkWorld1. Shaw, K. (6. oktober 2020) *What is a network switch and how does it work?*. Lokaliseret 14 maj på: https://www.networkworld.com/article/3584876/what-is-a-network-switch-and-how-does-it-work.html

NetworkWorld2. Shaw, K. (14. oktober 2020) *The OSI model explained and how to easily remember its 7 layers*. Lokaliseret d. 14 maj på: https://www.networkworld.com/article/3239677/the-osi-model-explained-and-how-to-easily-remember-its-7-layers.html

OSI-model (u.d.) *Network Layer*. Lokaliseret d. 14 maj på: https://www.osi-model.com/network-layer/

SMVdanmark (u.d.) *Seneste konkurstal*. Lokaliseret d. 10. april 2021 på: https://smvdanmark.dk/vi-tilbyder/corona-hjælpepakker-nyheder-links/seneste-konkurstal

Srivathsav, R. (15. oktober 2020) *A little more than the CIA triad!*. Lokaliseret d. 26 maj 2021 på: https://medium.com/coinmonks/a-little-more-than-the-cia-triad-6c54d6263083

Vestergård, G., L. (24 august 2010) *Hvad er videnskabsteori?* Lokaliseret d. 29. maj 2021 på: https://videnskab.dk/kultur-samfund/hvad-er-videnskabsteori

Welekwe, A (2021) *The Ultimate Guide to VPN Tunneling & How To Use It In 2021.* Lokaliseret den 18. Maj 2021 på: https://www.vpnmentor.com/blog/ultimate-guide-to-vpn-tunneling/ 23. maj 2021.