FORSTUDIE

Sikker ledelse og IT-sikkerhed

Startdato: 01-08-2024

Slutdato: 31-12-2024

Deltagere: Peter Thaysen (SmartLearning), Ove Thomsen (SmartLearning) og Daniel Ellebæk (Cphbusiness)

Indhold

Introduktion

I takt med at digitaliseringen accelererer, bliver IT-sikkerhed en stadig vigtigere prioritet for virksomheder i alle størrelser. Små- og mellemstore virksomheder (SMV'er) står dog overfor særlige udfordringer, når det gælder udarbejdelse og implementering af IT-politikker, -retningslinjer og -beredskabsplaner. Med begrænsede ressourcer og fokus på daglig drift kan det være svært for ledelsen i SMV'er at balancere mellem kortsigtede forretningsmål og langsigtede strategier for IT-sikkerhed.

Dette forstudie har til formål at identificere og kortlægge de centrale problemstillinger ved implementeringen af IT-sikkerhedsforanstaltninger i SMV'er, med særligt fokus på ledelsens rolle. Det er afgørende, at ledelsen forstår de økonomiske konsekvenser, som både en investering i og en mangel på IT-sikkerhedsforanstaltninger kan medføre. Samtidig øger lovgivningen kravene til IT-sikkerheden, hvilket gør det endnu vigtigere at sikre en effektiv implementering af relevante IT-sikkerhedspolitikker.

Gennem forstudiet vil vi undersøge eksisterende viden på området via litteraturstudier og samarbejde med organisationer og uddannelsesinstitutioner, der beskæftiger sig med IT-sikkerhed. Forventningen er, at vi gennem denne undersøgelse kan belyse, hvordan personlig ledelse påvirker virksomheders evne til at håndtere IT-sikkerhedsrisici. Studiet vil bidrage med værdifuld indsigt i, hvordan SMV'er kan styrke deres IT-sikkerhed gennem bedre ledelsespraksis og strategisk prioritering af IT-sikkerhedsforanstaltninger. Resultaterne vil danne grundlag for fremtidige projekter og potentielt udviklingen af kurser, der understøtter ledelsens ansvar for IT-sikkerheden.

Metode

Forstudiet har benyttet en induktiv forskningsmetode med inspiration fra Grounded Theory (Guvå, 2005), som vil sikre et eksplorativt og fleksibelt undersøgelsesdesign. Formålet var at afdække, hvordan ledelsen i små- og mellemstore virksomheder (SMV'er) forholder sig til IT-sikkerhed, samt hvordan de håndterer implementeringen af sikkerhedstiltag i praksis.

Dette blev gjort gennem et litteraturstudie, hvor relevante rapporter og analyser om IT-sikkerhed og ledelse blev gennemgået. Dertil foretog vi også et litteraturstudie af Danmarks Forskningsportal for at søge forskningslitteratur om koblingen mellem IT-sikkerhed og ledelse.. Dertil undersøgte vi hvad der var af relevante projektresultater fra EA Viden. Dette samlede litteraturstudie danner fundamentet for at identificere potentielle videngab[1]. Derudover vil resultaterne fra litteraturstudiet bruges til at forme konkrete forskningsspørgsmål.

Dataindsamlingen omfatter også et interview til supplement af litteraturstudiet, for at perspektivere det fundne.

Metodens styrke består i dens fleksibilitet og tilpasningsevne, hvilket gav mulighed for at justere undersøgelsesdesignet undervejs og sikre, at studiet forbliver fokuseret på at skabe et godt overblik over det valgte emne.

[1] **Videngab** refererer her til de områder, hvor den eksisterende forskning eller viden inden for et emne er utilstrækkelig eller mangelfuld, hvilket skaber muligheder for yderligere undersøgelser og nye opdagelser.

Oversigt over Empiriske Kilder om IT-sikkerhed i SMV'er: Blogs, Posts og Forskning

I dette afsnit præsenteres en oversigt over de empiriske kilder, der er anvendt til at belyse IT-sikkerheden i små og mellemstore virksomheder (SMV'er) i Danmark. Kilderne er opdelt i tre hovedkategorier: blogs og posts fra større virksomheder, rapporter og forskningsartikler. De første kilder repræsenterer en praktisk og erhvervsorienteret tilgang til cybersikkerhed, hvor virksomheder og organisationer deler deres erfaringer, udfordringer og anbefalinger. De to andre kategorier indeholder akademiske undersøgelser og officielle rapporter, der analyserer IT-sikkerheden i SMV'er gennem kvantitative og kvalitative data.

Denne inddeling giver et bredt og nuanceret indblik i de udfordringer og muligheder, som SMV'er står overfor, når det gælder implementeringen af sikkerhedsforanstaltninger. Afsnittet fremhæver både de praktiske tilgange fra erhvervslivet og de metodiske analyser fra forskningsverdenen, hvilket skaber en omfattende forståelse af IT-sikkerhedens rolle i danske SMV'er.

1. Blogs og posts fra større virksomheder

- SikkerDigital.dk. Digital sikkerhed i danske SMV’er 2021. Erhvervsstyrelsen, 2021. Tilgængelig fra: https://www.sikkerdigital.dk/virksomhed/publikationer/digital-sikkerhed-i-danske-smv%E2%80%99er-2021
- Industriens Fond. Cybersikkerhed hos SMV’er. Tilgængelig fra: https://industriensfond.dk/vores-fokusomrader/cybersikkerhed
- D-mærket. EU-strammer reglerne for cybersikkerhed med NIS 2 direktivet. Tilgængelig fra: https://www.d-maerket.dk/viden-og-vaerktoejer/artikler/brug-d-maerket-og-bliv-klar-naar-eu-strammer-reglerne-for-cybersikkerhed-med-nyt-nis2-direktiv
- SMV Danmark. Virksomhederne mangler rådgivning om digital sikkerhed. Tilgængelig fra: https://smvdanmark.dk/analyser/temaanalyser/virksomhederne-mangler-r%C3%A5dgivning-om-digital-sikkerhed

2. Rapporter

- Digitaliseringsstyrelsen. Digital sikkerhed i danske SMV’er 2023. Tilgængelig fra: https://digst.dk/media/29043/digital-sikkerhed-i-danske-smver-2023_endelig0310-a.pdf
- Deloitte. IT-sikkerhed og datahåndtering i danske SMV'er. Tilgængelig fra: https://digst.dk/media/31248/deloitte-it-sikkerhed-og-datahaandtering-i-danske-smver.pdf
- Dansk Industri. SMV'ernes IT-sikkerhed halter stadigvæk. Tilgængelig fra: https://www.danskindustri.dk/di-business/arkiv/nyheder/2023/10/smvernes-it-sikkerhed-halter-stadig/
- Danmarks Statistik. Øget cybersikkerhed i små virksomheder. Tilgængelig fra: https://www.dst.dk/da/Statistik/nyheder-analyser-publ/nyt/NytHtml?cid=54562

- Danmarks Statistik. Små virksomheder har mindre fokus på cybersikkerhed. Tilgængelig fra: https://www.dst.dk/da/Statistik/nyheder-analyser-publ/nyt/NytHtml?cid=50382

3. Forskningsartikler

- Assante, Dario [et al.] Cybersecurity Education for SMEs. 2023, Chapter, Conference Paper, Lecture Notes in Networks and Systems
- Falch M. [et al.] Cybersecurity Strategies for SMEs in the Nordic Baltic Region. 2022, Article, Journal of Cyber Security and Mobility
- Fleron, Camilla Nadja [et al.] Towards a Basic Security Framework for SMEs – Results From an Investigation of Cybersecurity Challenges in Denmark. 2023, Conference Paper, Proceedings Paper, 2023 IEEE 31st International Requirements Engineering Conference Workshops (REW)
- Wong, Wai Peng [et al.] A conceptual framework for information-leakage-resilience. 2021, Article, Annals of Operations Research
- Erhvervsakademi Kolding. Password behaviour: A threat to cyber security. A study of future financial sector employees in Denmark. Tilgængelig fra: https://www.eaviden.dk/project/password-behaviour-a-threat-to-cyber-security-a-study-of-future-financial-sector-employees-in-denmark/

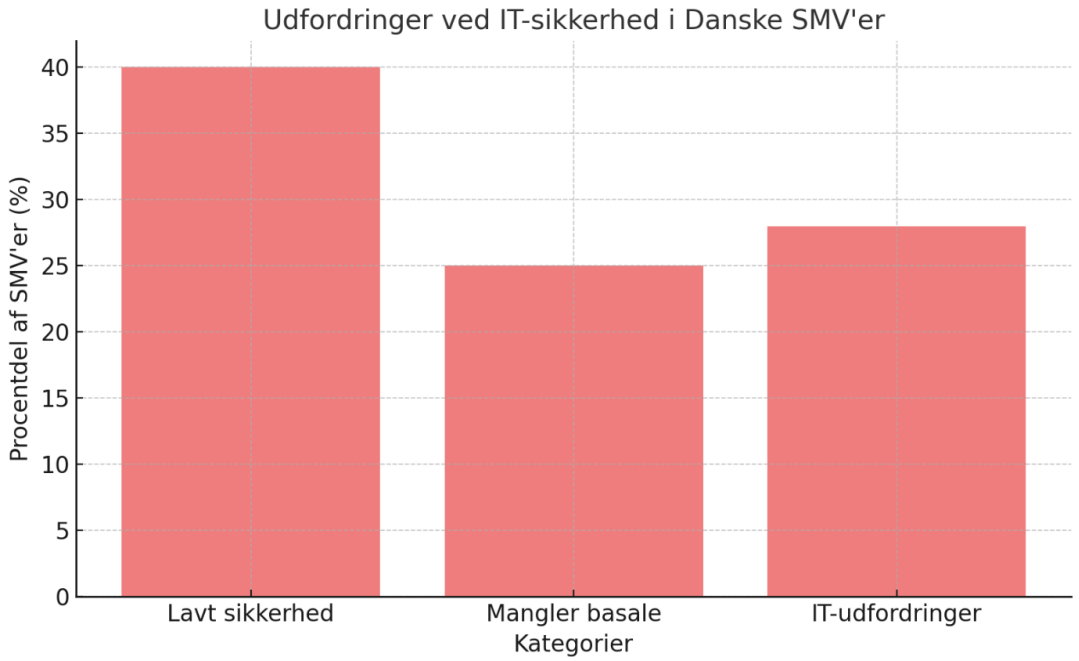
Udfordringer og muligheder ved implementering af IT-sikkerhed i danske SMV'er

De fleste af analyserne baserer sig på kvantitative metoder som spørgeskemaundersøgelser, hvor SMV'er bliver spurgt om deres brug af og udfordringer med IT-sikkerhed. For eksempel baserer rapporten fra Digitaliseringsstyrelsen sig på data fra Danmarks Statistiks årlige undersøgelse "IT-anvendelse i virksomheder" (VITA[2]), som indsamler svar fra tusindvis af virksomheder. Dataindsamlingen fokuserer på at afdække brugen af basale sikkerhedsforanstaltninger, såsom systemopdateringer og databeskyttelse. Kvalitative metoder i form af interviews bruges også til at forstå ledelsens tilgang til IT-sikkerhed i virksomhederne.

Et fællestræk i analyserne er, at 40-50% af SMV'erne har et utilstrækkeligt sikkerhedsniveau i forhold til deres risikoprofil. Omkring 28% af SMV'erne har udfordringer med at implementere IT-sikkerhedsløsninger, hovedsageligt på grund af manglende IT-kompetencer, økonomiske ressourcer og tvivl om værdien af IT-sikkerhedsinvesteringer. Desuden peger rapporter på, at en fjerdedel af SMV'erne ikke har implementeret de mest grundlæggende sikkerhedsforanstaltninger, såsom regelmæssige opdateringer og backup.

Ledelsen spiller en afgørende rolle i, hvordan IT-sikkerhed prioriteres i SMV'er. En af de største udfordringer er, at ledelsen ofte mangler forståelse for IT-sikkerhedens vigtighed og undervurderer konsekvenserne af sikkerhedsbrud. Flere af undersøgelserne fremhæver behovet for, at ledelsen involverer sig mere aktivt i at udarbejde og implementere sikkerhedsstrategier, herunder at forstå de økonomiske risici ved manglende IT-sikkerhed.

[2] **VITA** står for "IT-anvendelse i virksomheder", som er en årlig spørgeskemaundersøgelse fra Danmarks Statistik



Figur 1 - Udfordringer Ved IT-Sikkerhed I Danske SMV'er

Statistikken fra diagrammet Figur 1 giver os flere vigtige indsigter i IT-sikkerhedstilstanden i danske små- og mellemstore virksomheder (SMV'er):

1. **En stor andel af SMV'er har lavt sikkerhedsniveau** (40%): Dette indikerer, at mange SMV'er ikke har tilstrækkelige sikkerhedsforanstaltninger i forhold til deres risikoprofil. Det betyder, at mange virksomheder er sårbare over for cyberangreb, og der er behov for øget opmærksomhed på grundlæggende sikkerhedstiltag.
2. **Mangel på basale sikkerhedsforanstaltninger** (25%): Ca. en fjerdedel af SMV'erne har ikke implementeret de mest grundlæggende sikkerhedsforanstaltninger som regelmæssig opdatering af systemer og backup af data. Dette er et stort problem, da det gør dem særligt sårbare over for selv simple cybertrusler. Denne mangel kan også være et resultat af manglende viden eller ressourcer, hvilket understreger vigtigheden af uddannelse og rådgivning.
3. **Udfordringer med IT-sikkerhedsløsninger** (28%): Mange SMV'er oplever problemer med at anvende IT-sikkerhedsløsninger, og de peger især på mangel på IT-kompetencer og ressourcer. Dette understreger behovet for at gøre IT-sikkerhed mere tilgængelig og forståelig for mindre virksomheder, der måske ikke har specialiserede IT-afdelinger.

Læringspunkter:

- Uddannelse og rådgivning er nødvendigt for at forbedre sikkerhedsniveauet.
- Ressourcebegrænsninger hæmmer implementeringen af it-sikkerhedsforanstaltninger.
- Ledelsens engagement er afgørende for at sikre bedre IT-sikkerhed.

Samlet set viser statistikken, at der er et stort potentiale for forbedring inden for IT-sikkerhed i danske SMV'er, især når det gælder implementering af grundlæggende sikkerhedstiltag og opbygning af interne IT-sikkerhedskompetencer.

Ledelsens Rolle, Økonomiske Barrierer og Mangel på kompetencer

I takt med den stigende digitalisering af danske små- og mellemstore virksomheder (SMV'er) bliver IT-sikkerhed en afgørende prioritet. Dog står mange SMV'er over for betydelige udfordringer, når det kommer til at implementere og vedligeholde en robust IT-sikkerhedsstruktur. Ledelsens rolle er central i denne sammenhæng, men de økonomiske barrierer og manglen på IT-kompetencer skaber ofte hindringer for den nødvendige sikkerhedsindsats. I dette afsnit vil vi diskutere, hvordan ledelsen kan påvirke IT-sikkerheden, hvilke økonomiske udfordringer de står overfor, samt hvordan mangel på IT-kompetencer kan hæmme fremdrift og sikkerhed.

Ledelsens rolle i IT-sikkerhed

Ledelsen i en SMV har en afgørende funktion i at sætte dagsordenen for IT-sikkerhed. Ledelsen er ansvarlig for at fastlægge virksomhedens IT-sikkerhedspolitik og beslutte, hvordan ressourcer skal allokeres for at beskytte virksomheden mod trusler. I mange SMV'er er IT-sikkerhed desværre ofte ikke en topprioritet, da ledelsen kan undervurdere risikoen for cyberangreb eller datatab. Dette skyldes delvis en opfattelse af, at mindre virksomheder ikke er attraktive mål for hackere, hvilket dog ikke er tilfældet. Cyberkriminelle retter sig ofte mod mindre virksomheder, netop fordi de antager, at sikkerheden er lavere, og dermed lettere at bryde igennem.

Ledelsen skal være bevidst om, at IT-sikkerhed ikke kun handler om tekniske foranstaltninger, men også om at skabe en kultur, hvor alle medarbejdere forstår og tager ansvar for sikkerheden. Netop kobling mellem individ og organisation er et svagt punkt når det kommer til IT-sikkerhed. Ved at involvere medarbejderne i træning og bevidstgørelsesinitiativer kan ledelsen reducere risikoen for brud, der opstår som følge af menneskelige fejl. Dette kræver dog, at ledelsen dedikerer tid og ressourcer til at opbygge et fundament af viden og praksis i virksomheden.

Ledelsen er bærer af informationssikkerhedskultur og det er afgørende for at mindske risiciene for it-sikkerhedsbrud. Det indikeres at der er tale om et misforhold mellem opfattelsen af sikkerhedsudfordringer og ansvar af den øverste ledelse. Dette udgør en barriere for at sikre, at medarbejderne har nødvendige kompetencer til implementering af it-sikkerhed og sikkerhedsforanstaltninger, og at de får en ordentlig mulighed for at gøre det. Dette har meget at gøre med den rolle, lederen spiller. Derimod fandt vi ikke noget der kobler de personlige ledelsesopgaver direkte til IT-sikkerhed, så skal den vinkel udforskes nærmere, kræver det at vi selv opstiller og undersøger det fra bunden.

Økonomiske barrierer for IT-sikkerhed

En af de største udfordringer, som mange SMV'er står over for, er de økonomiske barrierer for IT-sikkerhed. For en mindre virksomhed kan det virke uoverkommeligt at investere i dyre sikkerhedsløsninger, såsom avanceret antivirus-software, firewalls, kryptering, samt løbende opdateringer af systemer. De økonomiske omkostninger ved IT-sikkerhed skal ofte vejes op mod andre presserende behov, såsom drift og vækst.

For at tackle de økonomiske udfordringer kan ledelsen overveje en risikobaseret tilgang, hvor IT-sikkerheden tilpasses virksomhedens specifikke risikoprofil og behov. I stedet for at investere i de dyreste løsninger kan ledelsen prioritere de mest nødvendige sikkerhedsforanstaltninger, såsom backup, softwareopdateringer og adgangsstyring. Desuden kan offentlige tilskud og puljer, som f.eks. SMV, udnyttes til at få økonomisk støtte til implementeringen af IT-sikkerhedsløsninger. Ved at udnytte sådanne muligheder kan selv mindre virksomheder opnå en grundlæggende beskyttelse uden at sprænge budgettet.

Mangel på IT-sikkerheds kompetencer i SMV'er

En anden væsentlig udfordring er manglen på IT-sikkerhedskompetencer internt i mange SMV'er. I mange tilfælde har virksomhederne ikke dedikerede IT-afdelinger, og de teknologiske beslutninger ligger ofte hos ledelsen eller enkelte medarbejdere, der ikke har dybdegående kendskab til IT-sikkerhed. Denne mangel på viden og kompetencer gør det vanskeligt for SMV'er at identificere risici, implementere passende sikkerhedsløsninger og reagere korrekt på sikkerhedshændelser. I stedet for at proaktivt forebygge sikkerhedsproblemer ender mange SMV'er med at reagere reaktivt, når skaden allerede er sket.

For at overvinde denne udfordring kan ledelsen tage en række skridt. En oplagt løsning er at outsource IT-sikkerheden til eksterne specialister. Der findes mange virksomheder, der tilbyder skræddersyede sikkerhedsløsninger for SMV'er, herunder administration af sikkerhedssoftware, overvågning af netværkstrafik og rådgivning om best practice. Outsourcing kan være en omkostningseffektiv løsning for virksomheder, der ikke har ressourcerne til at opbygge en intern IT-afdeling.

Alternativt kan ledelsen investere i at opkvalificere deres medarbejdere. Dette kan gøres gennem kurser i grundlæggende IT-sikkerhed eller ved at deltage i awareness-programmer, der styrker medarbejdernes evne til at identificere og håndtere trusler. Samarbejde med uddannelsesinstitutioner eller erhvervslivets IT-netværk kan også give ledelsen adgang til ressourcer og viden, som ellers ville være sværere at opnå internt.

Forslag til løsninger

For at adressere de udfordringer, der knytter sig til IT-sikkerhed i SMV'er, kan ledelsen implementere følgende tiltag:

1. Prioritere IT-sikkerhed på strategisk niveau ved at integrere det som en del af virksomhedens langsigtede planlægning.
2. Udnytte offentlige tilskud og andre støtteordninger til at reducere de økonomiske barrierer for investering i sikkerhedsløsninger.
3. Opkvalificere medarbejdere gennem træning og awareness-programmer, så alle i virksomheden forstår deres rolle i at sikre en sikker digital adfærd.
4. Regelmæssige sikkerhedsrevisioner for at identificere og løse eventuelle sikkerhedshuller, før de bliver til reelle trusler.
5. Udvikle retningslinjer og planer, der ikke kun er designet til at tackle et bestemt problem, såsom ny lovgivning eller seneste krise, men som er tilpasningsdygtige nok til at blive anvendt løbende og kunne tage højde for en række fremtidige ændringer

Konklusion

IT-sikkerhed er en blivende udfordring for danske små- og mellemstore virksomheder (SMV'er), hvor ledelsen skal spille en central rolle i at sikre virksomhedens digitale beskyttelse. Selvom mange SMV'er står over for økonomiske barrierer og mangel på interne IT-kompetencer, er det afgørende, at ledelsen tager ansvar for at implementere passende sikkerhedsløsninger og skabe en kultur, hvor sikkerhed er en prioritet. Involveret og ansvarlig ledelse i forbindelse med sikkerhedsbeslutninger er centralt for succesen af disse beslutninger, ideelt set med den øverste ledelse i spidsen virksomhedens it-sikkerhedsforanstaltninger.

Økonomiske begrænsninger gør det vanskeligt for mange SMV'er at investere i avancerede sikkerhedsløsninger, hvilket ofte fører til, at basale sikkerhedsforanstaltninger overses. Manglen på IT-sikkerhedsfaglige kompetencer forværrer situationen, da mange virksomheder ikke har den nødvendige viden til at identificere og håndtere sikkerhedsrisici. Dette understreger behovet for ledelsesmæssigt at tage ansvar for området og sikre at eks. en økonomisk begrænsning ikke i virkeligheden er en manglende vilje.

Ledelsen bør tage proaktive skridt ved at udarbejde klare beredskabsplaner, IT-sikkerhedspolitikker og -retningslinjer, gennemføre regelmæssige sikkerhedsrevisioner og investere i træning af medarbejdere. Ved at udnytte offentlige tilskud og eventuelt outsource kritiske funktioner kan SMV'er løse mange af de økonomiske og kompetencemæssige udfordringer, der hæmmer IT-sikkerheden. En stærkere ledelsesmæssig involvering vil ikke kun reducere risikoen for cyberangreb, men også beskytte virksomhedens omdømme, sikre kundetillid og skabe en robust digital infrastruktur.

Samlet set viser analysen, at selvom IT-sikkerhed i SMV'er kan være udfordrende, kan ledelsens engagement og strategiske prioritering skabe væsentlige forbedringer. Ved at adressere økonomiske barrierer og kompetencehuller kan SMV'er opnå et højere sikkerhedsniveau og dermed bedre ruste sig mod fremtidens digitale trusler. Men den afsøgte litteratur peger ikke nærmere ind i hvordan lederen så skal *agere* - selv om lederen gøres til en afgørende aktør.

Forslag til handling

Der er et markant videnshul i forhold til ledelsesperspektivet og udmøntningen af it-sikkerhedsperspektivet i SMV'er. Mange små og mellemstore virksomheder mangler en dybdegående forståelse af, hvordan ledelsen kan og bør integrere it-sikkerhed i deres overordnede strategiske planer. Vi peger på, at ledelsen har en rolle, de ikke udfylder, og at dette skyldes, at perspektiver på økonomi og ressourcer/kompetencer tager præcedens i ledelsens overvejelser.

Det skal undersøges, hvilken rolle lederen skal indtage for at sikre succes med IT-sikkerhedsbeslutninger. Det er afgørende at forstå, hvordan ledelsens engagement og aktive deltagelse kan påvirke effektiviteten af disse beslutninger. Således er det personlige ledelsesengagement båret af den rolle, lederen spiller i forhold til beslutningerne. Lederen skal ikke kun være en beslutningstager, men også en aktiv fortaler for IT-sikkerhed, der fremmer en kultur, hvor IT-sikkerhed prioriteres på alle niveauer i organisationen. Dette indebærer, at lederen skal være velinformeret om de nyeste trusler og sikkerhedspraksisser samt være i stand til at kommunikere vigtigheden af IT-sikkerhed til alle medarbejdere. .

Perspektivering

Vores perspektivering er baseret på et interview med Malene Stidsen, Programchef for Industriens Fonds Cybersikkerhedsprogram. I løbet af interviewet spurgte vi ind til Malenes erfaringer med de problemstillinger vi har arbejdet med i løbet af forprojektet (interviewet blev gennemført sent i forløbet og kunne derfor bruges til at kaste yderligere lys over vores arbejde). Generelt kunne vi få bekræftet hvor ressourcer, kompetencer og tid har indflydelse på hvordan især SMV'er tilgår IT-sikkerhed. Men i relation til ledelse fandt vi to interessante indfaldsvinkler: Lederens rolle og forbindelsen til forretningsmodellen.

For lederen er det vigtigt at være rollemodel i forhold til IT-sikkerhed. Det gælder for lederen selv at praktisere den awareness som ønskes i virksomheden, og selv være engageret og vidende om IT-sikkerhed. Den centrale IT-sikkerhedsudfordring handler om samarbejde. Altså samarbejde mellem leder og medarbejdere om IT-sikkerhed. Ledelsen skal gå forrest og være kulturbærer og bakke IT-medarbejderen op.

Der er også et andet samarbejde som er vigtigt. Mange ledere betragter IT-sikkerhed som en udgift, der først prioriteres, når en hændelse allerede har fundet sted, hvilket kan have alvorlige konsekvenser. Et cyberangreb kan have alvorlige økonomiske konsekvenser, herunder tab af kundedata, skader på omdømmet og direkte finansielle tab, hvilket i sidste ende kan true virksomhedens overlevelse.

IT-sikkerhed er ikke alene en beskyttelsesforanstaltning; et højt niveau af IT-sikkerhed i en virksomhed kan også fungere som en konkurrenceparameter, især i B2B-sammenhænge. Når virksomheder handler med andre virksomheder, bliver robust IT-sikkerhed sandsynligvis et fremtidigt afgørende kriterium for valg af samarbejdspartnere. En virksomhed, der kan dokumentere en stærk IT-sikkerhedsprofil, har en klar fordel i forhold til salg og underleverancer, da det skaber tillid og reducerer risikoen for samarbejdspartnere i forsyningskæden. Med risiko menes blandt andet sikker udveksling og lagring af data. Det er vigtigt at lederen lader IT-medarbejderne forstå koblingen og hjælper dem med at sætte forretningssprog på IT-sikkerheden så det ikke kun fortaber sig i teknik.

Potentielle forskningsspørgsmål

Hvilken lederrolle er nødvendig for at sikre en succesfuld IT-sikkerhedskultur?

Hvordan kobles lederens personlige ledelsesopgaver til virksomhedens IT-sikkerhed?

Hvordan kan lederen fremme forståelsen for IT-sikkerhed som en forretningskomponent?

Hvordan kan IT-sikkerhed forankres i ledelsesansvaret?

Bibliografi

Guvå, G. &. (2005). *Grundad teori: Ett teorigenererande forskningsperspektiv. Studentlitteratur.*