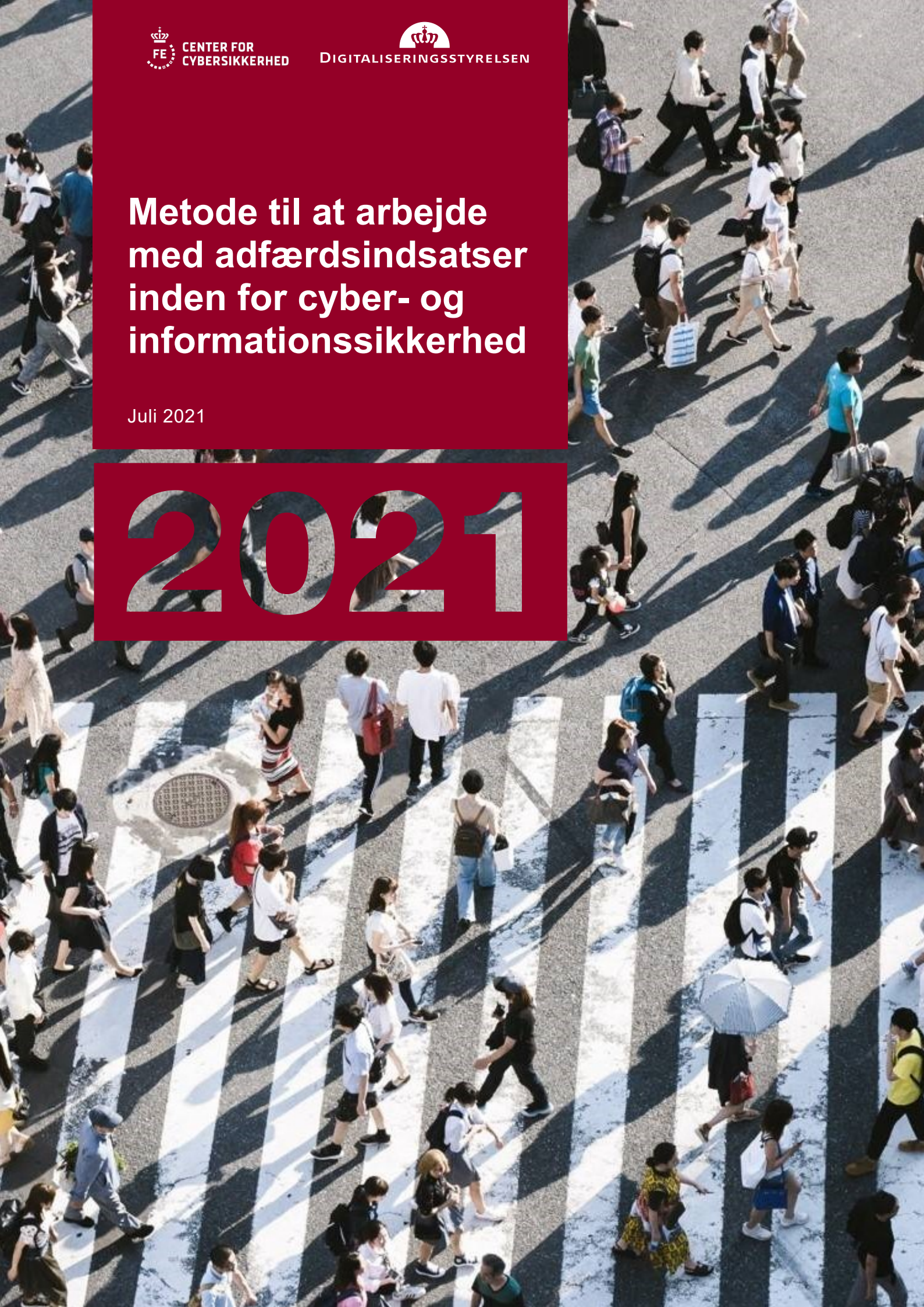


Metode til at arbejde med adfærdsindsatser inden for cyber- og informationssikkerhed

Juli 2021

2021



Indholdsfortegnelse

1. Indledning	3
Formål	3
Målgruppe	4
Hvad er adfærd?	5
Etiske overvejelser	5
Læsevejledning	5
2. Metode	6
Fase 1: Identificer problemerne og sæt mål for ønsket adfærd	6
Fase 2: Analyser og diagnosticer adfærdsproblemet	7
Fase 3: Udarbejd en adfærdsindsats	9
Fase 4: Test adfærdsindsatsen	13
Fase 5: Implementer adfærdsindsatsen og følg op	15
3. Afrunding	17
4. Referencer	18
5. Bilag 19	
Case: Adfærdsproblem med ulåste pc'er	19

1. Indledning

Internationale undersøgelser anslår, at størstedelen af alle hackerangreb og informationssikkerhedsbrud skyldes menneskelige fejl¹. Samme konklusion har det danske Datatilsyn fremført².

Derfor skal organisationer tage højde for det menneskelige aspekt, når organisationens samlede informationssikkerhed skal styrkes. Det er ikke nok at nedskrive informationssikkerhedsretningslinjer og gøre ansatte opmærksomme på, at de er ansvarlige for at efterleve dem, for det bliver ikke nødvendigvis vekslet til reel styrket sikkerhed. En reel styrkelse af informationssikkerheden må involvere at informationssikkerhedspolitikker og –retningslinjer reelt efterleves ved at designe indsatser, der styrer ansattes adfærd i en ønskelig sikker retning.

Har du genbrugt eller nedskrevet dit password? Har du haft til hensigt at opdatere din pc inden arbejdsdagens udgang, men alligevel er det stadig ikke sket ugen efter? Eller bruger du trådløse, usikre netværk, når du er på farten? I så fald er du ikke den eneste. Faktisk handler alle mennesker dagligt imod deres viden og gode hensigter.

Formål

Vejledningen beskriver, hvordan organisationer kan identificere og analysere adfærdsproblemer relateret til organisationens informationssikkerhed med henblik på at implementere adfærdsindsatser i organisationen. Adfærdsproblemer kan eksempelvis være håndtering af phishing e-mails, brugen af usikre netværk eller svage passwords.

Vejledningen præsenterer en metode, der er baseret på *best practice* til at arbejde systematisk med adfærd gennem fem faser:

¹ Hill, Michael: 90% of UK Data Breaches Due to Human Error in 2019, Infosecurity Magazine.
M., Jacob: Human error is still the number one cause of most data breaches in 2021, Influencive
² Datatilsynets statistikbank over fordeling af hændelser

Figur 1:

Adfærdsindsatsers fem faser



Den præsenterede metode er inspireret af og baseret på OECD's *The BASIC Toolkit*³, der er *best practice* på området. Metoden, der er udviklet til arbejde med adfærd i offentlig politikudvikling, er her tilpasset arbejdet med informationssikkerhed og væsentligt forkortet med det formål at lave en overskuelig, målrettet og handlingsanvisende vejledning. Udgangspunktet er adfærdsændring på informationssikkerhedsområdet. Dog kan den anvendte metode også benyttes i andre sammenhænge. For teoretisk afsæt, yderligere metodebeskrivelser og –tiltag samt referencer henvises til det fulde BASIC-rammeverk. Her findes der også beskrivelser af andre metoder til at arbejde med adfærdsindsatser.

Vejledningen tilbyder ikke en færdig pakkeløsning til at skabe adfærdsforandrende tiltag, men præsenterer en metode baseret på teori og *best practice* til at arbejde evidensbaseret og datadrevet med adfærd. I metoden præsenteres dog også konkrete værktøjer, såkaldte greb, til at ændre en uønsket adfærd. I bilag 1 eksemplificeres og konkretiseres metoden i en case.

Målgruppe

Vejledningen er målrettet CISO'er (Chief Information Security Officer) og de medarbejdere, der arbejder med informationssikkerhed i såvel offentlige som private organisationer. I det konkrete adfærdsarbejde vil det ofte være relevant at inddrage andre

³ Tools and Ethics for Applied Behavioural Insights: The BASIC Toolkit

faggrupper og afdelinger ligesom, det er essentielt, at indsatsen er forankret i ledelsen, da en adfærdsindsats kræver tid og ressourcer.

Hvad er adfærd?

Adfærd handler grundlæggende om, når mennesker agerer på én måde frem for en anden, også når der ageres uhensigtsmæssigt, og et adfærdsproblem opstår. I en informationssikkerhedskontekst defineres et adfærdsproblem som:

'Et adfærdsproblem i en informationssikkerhedskontekst er et uhensigtsmæssigt adfærdsmønster (valg, handling eller vurdering), der øger organisationens sårbarhed overfor cybertrusler. Adfærdsmønstret forekommer på trods af, at man har god grund til at gøre noget andet. Man har altså information, holdninger, incitament og eventuelt regulering, der sammen giver tilstrækkelig anledning til en anden adfærd' ⁴

Det er vigtigt at holde sig for øje, at adfærdsindsatser ikke er det samme som awareness-tiltag, da adfærd alene drejer sig om menneskers faktiske handlinger eller fravalg heraf. Lidt forsimplet kan man sige, at det er et vidensproblem, hvis en medarbejder ikke ved, hvordan hun skal opdatere sin pc. Et problem, der handler om manglende awareness. Men hvis hun godt ved, hvordan hun opdaterer pc'en og kender deadline, men alligevel ikke får det gjort, er der tale om et adfærdsproblem. En medarbejder skal altså have erfaring med eller viden om et område for at kunne have en ønsket adfærd. Prioritering af uddannelse og træning af medarbejdere er derfor essentielt for, at viden bliver omdannet til kompetencer.

Etiske overvejelser

Adfærd handler om mennesker, og derfor bør etiske overvejelser altid indgå i planlægningen af en adfærdsindsats. Det er blandt andet overvejelser om indsamling og opbevaring af data på individ- såvel som gruppeniveau. Formålet med en adfærdsindsats er at ændre adfærden i organisationen, ikke at udstille enkelte individers uhensigtsmæssige adfærd⁵.

Læsevejledning

Vejledningen beskriver en metode til at arbejde med adfærd relateret til informationssikkerhed, der består af fem faser. I det følgende beskrives hver enkelt af metodens faser. Først beskrives fasens formål fulgt af beskrivelse af de tiltag og overvejelser, der bør gennemføres. Vejledningens Bilag 1 er en case, hvor de enkelte faser eksemplificeres.

⁴ Egen oversættelse af den generelle definition af et adfærdsproblem i Tools and Ethics for Applied Behavioural Insights: The BASIC Toolkit

⁵ En række parter har udgivet 'Kodeks for gennemførelse af sikkerhedstests', som med fordel kan læses i forbindelse med gennemførelse af en adfærdsindsats. Den guider til, hvordan sikkerhedstests generelt udføres med respekt for de etiske rammer og medarbejdernes hverdag og privatliv.

2. Metode

Fase 1: Identificer problemerne og sæt mål for ønsket adfærd

Informationssikkerhedsproblemer kan løses på flere måder og med forskellige værktøjer. Først og fremmest skal det derfor undersøges, om der faktisk er tale om et adfærdsproblem, der kræver en adfærdsindsats.

Adfærdsproblemet tydeliggøres ved at beskrive et adfærdsmønster. Her beskrives den aktuelle uønskede adfærd, hvem der udfører handlingen, hvornår, hvor, hvor ofte, og hvilken adfærd, der ønskes i stedet. Nedenstående tjekspørgsmål kan være til inspiration:

- ✓ Hvor foregår adfærden?
- ✓ Hvornår foregår adfærden?
- ✓ Hvem udfører adfærden?
- ✓ Hvor ofte udføres adfærden?
- ✓ Hvilke forskellige valgmuligheder har målgruppen tilgængelig, når sikkerhedsvalget træffes?
- ✓ Hvilken effekt har konteksten på adfærden? Herunder kollegaer, teknologiske løsninger, organisationskultur, indretning.

Både den aktuelle, uønskede adfærd og den ønskede adfærd beskrives som en handling. I arbejdet med adfærd er det ofte det uhensigtsmæssige handlemønster i en specifik situation, der vil definere og afgrænse målgruppen. Det står i modsætning til eksempelvis kommunikationsindsatser, hvor målgruppen oftest fastlægges ud fra beskrivende karakteristika. En adfærdsindsats kan målrettes alle medarbejdere i en organisation, der udfører den uønskede adfærd uagtet stilling, køn, afdeling, alder etc. Målgruppen kan således være alle medarbejdere, der eksempelvis genbruger deres passwords. Ideelt set anvendes observationsstudier til at afklare spørgsmålene. I de tilfælde, hvor det ikke er muligt, kan hyppigheden skønnes på baggrund af tilgængelig data.

I arbejdet med at komme nærmere den konkrete adfærdsindsats, der skal implementeres, kan organisationen på baggrund af den ønskede adfærdsændring formulere en SMART-målsætning, som kan være rammesættende for arbejdet. SMART-målsætningen vil endvidere benyttes i arbejdet med at evaluere og følge op på adfærdsindsatsen senere i forløbet.

- **Specifikt** – hvad ønskes opnået og for hvem?
- **Målbart** – hvordan måles, om adfærdsindsatsen er i mål?
- **Accepteret** – hvilken værdi opnås med adfærdsindsatsen?

- **Realistisk** – har organisationen de nødvendige ressourcer til at gennemføre adfærdsindsatsen inden for tidsperioden?
- **Tidsbestemt** – hvornår skal adfærdsindsatsen være implementeret?

Formålet med den første fase er således at identificere adfærdsproblemet, eksempelvis at medarbejdere ikke låser deres pc, når de forlader den samt formulere den ønskede adfærd. En organisation kan godt opleve flere adfærdsproblemer på samme tid, hvorfor organisationen med fordel kan sætte ind dér, hvor en indsats kan gøre den største forskel. Udvælgelsen af områder kan ske på baggrund af organisationens risikostyringsproces. Dette er en strategisk beslutning, som ledelsen i organisationen typisk vil være inddraget i. I næste fase undersøges årsagerne til problemet.

Fase 2: Analyser og diagnosticer adfærdsproblemet

Formålet med analysefasen er at analysere og diagnosticere, hvorfor den uønskede adfærd finder sted. Den uønskede adfærd analyseres ved hjælp af fire generelle adfærdsindsigter, der bidrager med dokumenteret viden om, hvordan mennesker handler i praksis. Det vil sige, hvad mennesker egentlig gør, og ikke hvad de siger, de gør. Indsigterne omhandler 1) menneskers begrænsede opmærksomhed, 2) hvordan mennesker danner formodninger, 3) hvordan mennesker træffer valg og 4) hvordan mennesker har svært ved at fastholde en bestemt adfærd over tid. Med afsæt heri opstilles hypoteser for, hvorfor den uønskede adfærd finder sted, evidens søges i eksisterende data eller i relevant litteratur, hvorefter der gennemføres en test af adfærden, der har til formål at validere og udfordre hypoteserne.

Opstil hypoteser

Hypoteser er påstande om virkeligheden, som kan undersøges og testes. For at kunne opstille disse hypoteser gennemgås de fire generelle adfærdsindsigter, der forklarer typiske områder af adfærdsproblemer og dermed bidrager til at formulere hypoteserne om, hvorfor den uønskede adfærd finder sted.

Fire generelle adfærdsindsigter

Opmærksomhed

Menneskers opmærksomhed er begrænset, og mennesker bliver let distraheret, overvældet og uopmærksomme. Adfærdsvidenskaben har kortlagt fem forskellige former for uopmærksomhed, som kan føre til et givent adfærdsproblem; når mennesker glemmer, overser noget, nedprioriterer en handling, multitasker og endelig, når mennesker bliver distraheret. Det betyder også, at mennesker kun kan fokusere på én ting ad gangen, og det er ikke altid det mest oplagte, rationelle eller hensigtsmæssige, der får opmærksomheden.

Formodningsdannelse

Formodningsdannelse handler om, hvordan mennesket skaber mening i verden. En formodning er en sindstilstand, hvor en person tror, at noget er tilfældet uanset, om

de har empirisk belæg for det eller ej. Mennesker har en tendens til at støtte sig til et sammenhængende verdensbillede, som bruges til at skabe mening, træffe beslutninger og forudse fremtidige begivenheder. Bliver de præsenteret for information, der går imod deres formodninger, vil informationen ofte blive ignoreret eller forkastet. Omvendt vil information, der bekræfter eksisterende holdninger, ofte blive fremhævet og tillagt øget værdi. Det betyder, at konsekvenser af handlinger ofte over- eller undervurderes, relevant information ikke inddrages, og at valg i høj grad baseres på simple mentale genveje frem for en nøje afvejning af al relevant information om et givent emne. Genvejene kan føre til fejlslutninger, men samtidig er de uundværlige, da mennesker ellers skulle behandle alle input rationelt og bevidst, hvilket der ikke er 'båndbredde' til.

Valg

Adfærdsvidenskaben har vist, at mennesker ikke foretager valg ud fra rationelle parametre og personlige præferencer alene. Ofte vil irrationelle parametre og psykologiske faktorer påvirke valgprocessen. Det kan eksempelvis dreje sig om tvivl eller fortrydelse, at mennesker foretrækker status quo samt påvirkes af fremstilling og præsentation af valgmulighederne. Når mennesker skal træffe valg, er de ofte påvirket af såkaldte bias, der er systematiske afvigelser fra rationelle normer.

Vedholdenhed

Det at træffe og udføre et valg er ikke nok til at fastholde den valgte adfærd over længere tid. Mennesker har vanskeligt ved at fastholde motivationen til langsigtede mål, hvis målene er i konflikt med andre ønsker. Selvregulering af adfærd er derfor nødvendigt, når langsigtede mål støder sammen med nutidige ønsker.

Når hypoteserne er opstillet på baggrund af adfærdsindsigterne, skal det undersøges, om de holder vand eller ej. Altså om de kan afvises eller bekræftes. Jo mere en hypotese kan underbygges, jo større er sandsynligheden for, at den er valid. Der er dog altid en risiko for, at en hypotese kan blive afvist i fremtiden. Hypoteserne afprøves ved hjælp af eksisterende data, evidens om den aktuelle adfærd.

Dataindsamling

Adfærdsanalysens fundament er en grundig dataindsamling, der kortlægger den nuværende adfærd. Dataindsamlingen vil ofte basere sig på en række forskellige metoder. Valget af metoder afhænger af ressourcer og den adfærd, der undersøges. Det kan eksempelvis ske ved at indsamle tilgængelige data, som kan give en forståelse for målgruppens nuværende adfærd. Det kan ske gennem desk research og kvantitative data om adfærden, der allerede er til rådighed, eksempelvis e-mails, supporthenvendelser og logfiler. En anden metode kan være at observere, hvad målgruppen gør og i hvilken kontekst. Det kan eksempelvis være ved at observere målgruppens adfærd i den faktiske kontekst, når den uønskede adfærd finder sted, hvor også eventuelle eksterne påvirkninger kan observeres.

Herefter bør den indsamlede data struktureres og bearbejdes. Samtidig bør hypoteserne sammenholdes med de indsamlede data og forkastes eller bibeholdes i det videre arbejde. Husk også her at genbesøge SMART-målsætningen for at se, om den bør justeres på baggrund af nye indsigter.

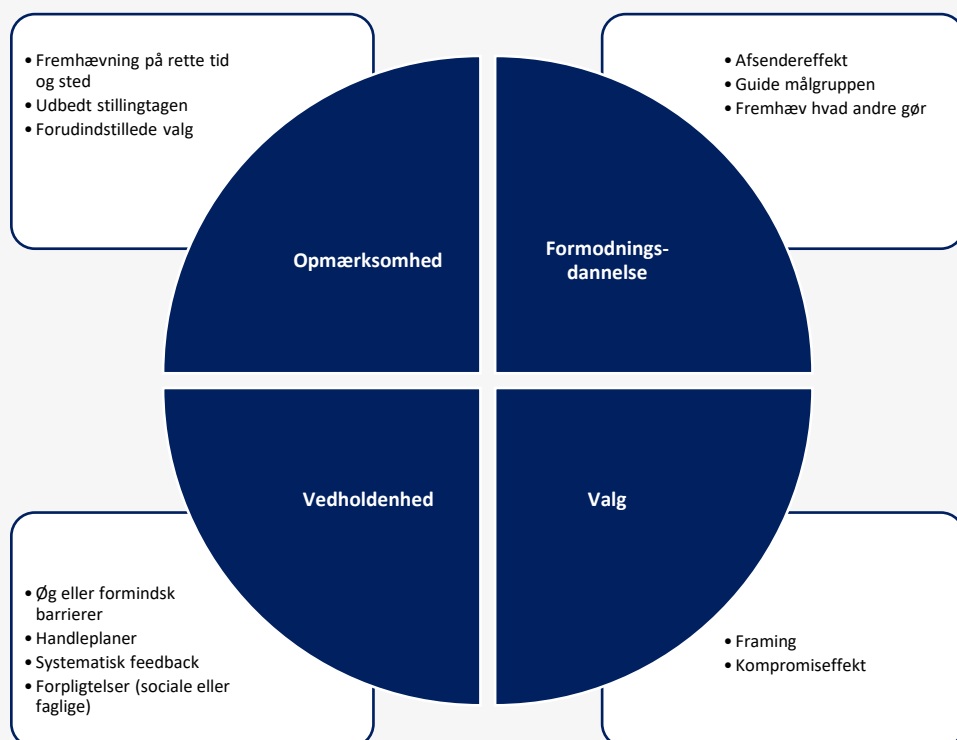
Analysefasen er en iterativ proces så i takt med, at der indsamles data og dermed indsigter om adfærden, kan der være behov for at udføre trinene flere gange.

Fase 3: Udarbejd en adfærdsindsats

Formålet med fase 3 er at udvælge den bedste adfærdsindsats til at opnå den ønskede adfærd. De konkrete tiltag eller værktøjer kaldes her for greb, der kan bruges til at opnå en ønsket adfærd. Grebene beskrives nedenfor under de fire generelle adfærdsindsigter, som hver især kan føre til et adfærdsproblem. Adfærdsindsatsen kan bestå af et eller flere greb afhængig af det identificerede problem.

Figur 2:

Adfærdsindsatsers greb afhængigt af identificeret adfærdsproblem



Problem: Opmærksomhed

Hvis analysefasen har vist, at det aktuelle adfærdsproblem skyldes manglende opmærksomhed, kan der arbejdes på en adfærdsindsats, der gør den ønskede adfærd relevant, eller hvor opmærksomheden henledes på den ønskede adfærd. Mennesker

er mere tilbøjelige til at fokusere på noget, når det præsenteres på en relevant måde. Det betyder, at adfærdsindsatsen skal ske på det rette sted og på det tidspunkt, hvor målgruppen er mest motiveret for at udføre den ønskede adfærd. Hvis målet er at få medarbejdere til at opdatere deres pc, kan en hypotese være, at de er mindre motiverede til at gøre det om morgenen. De er måske lige mødt på arbejde og har en travl dag foran sig. Lige før frokost kan derimod være et godt tidspunkt, hvor pc'en alligevel ikke bliver brugt. Det samme gælder for valg af sted. Det kunne eksempelvis være mere sandsynligt, at medarbejderne opdaterer pc'en i tide hjemmefra frem for på kontoret. Tidspunkt og placering af adfærdsindsatsen er derfor afgørende for, om adfærdsindsatsen opleves som relevant for målgruppen og dermed tiltrækker deres opmærksomhed. Menneskers evner og motivation er ikke konstante, og de træffer systematisk irrationelle beslutninger, når de er sultne, trætte eller stressede. Det er værd at holde for øje, når adfærdsindsatsen planlægges og udføres.

Man kan designe en indsats, der leder folks opmærksomhed hen på den ønskede handling. Konkret kan følgende greb bidrage til at gøre den ønskede adfærd relevant og dirigere medarbejdernes opmærksomhed mod den

Fremhævning på rette tid og sted

En måde at tiltrække opmærksomhed på er at fremhæve det relevante beslutningspunkt, eksempelvis ved at skabe kontrast til konteksten ved hjælp af størrelse, farver, former og bevægelse. Når et beslutningspunkt er fremhævet og fremtrædende, fanger det opmærksomheden og øger dermed sandsynligheden for, at det ønskede vælges. Ligeledes kan der arbejdes med at gøre uønskede valg mindre synlige. Endelig kan også arbejdes med at, at beslutningspunktet fremhæves på en bestemt placering på et bestemt tidspunkt, hvor målgruppen er mest motiverede for at tage stilling til den ønskede handling.

Udbedt stillingtagen

Der kan også arbejdes med at tiltrække opmærksomhed ved aktivt at få målgruppen til at tage stilling til den ønskede handling ved hjælp af såkaldte prompts (tvungen stillingtagen fra målgruppen), påmindelser eller pop-up beskeder, der henleder opmærksomheden på at skifte passwords, opdatere pc eller ved forsøg på at uploade filer til en ikke godkendt fildelingstjeneste etc. Her er det vigtigt, at prompts og/eller påmindelser hjælper medarbejderen med den handling, hun er i gang med. Ellers vil de ofte blive ignoreret.

Forudindstillede valg

Hvis målgruppen systematisk ikke er opmærksom på at udføre den ønskede handling, kan der i stedet arbejdes med forudindstillede valg, også kendt som defaults. Når det forudindstillede valg medfører den ønskede adfærd, vil den automatisk ske, når folk er uopmærksomme. Valget er allerede taget. Hvis indkomne mails med vedhæftninger, eksempelvis excel-filer med makroer, vurderes at udgøre en risiko for organisationen, kan deaktivering af makroer derfor sættes som default. Så er makroer automatisk deaktiveret, når folk er uopmærksomme, og den enkelte medarbejders

manglende uopmærksomhed udgør således ikke et problem. Individets valg påvirkes eller fratages ved sådanne greb, og de bør derfor anvendes med omtanke.

Problem: Formodningsdannelse

Hvis analysefasen har vist, at det aktuelle adfærdsproblem skyldes medarbejdernes formodningsdannelse, kan adfærdsindsatsen inddrage greb, der adresserer menneskers brug af mentale genveje, når de skal træffe valg. Mentale genveje er ofte forenkede og fejlbarlige og kan derfor føre til en uønsket adfærd. Den ønskede adfærd kan tilskyndes ved at arbejde med målgruppens mentale genveje, der ligger til grund for den uønskede adfærd.

Et eksempel på formodningsdannelse er i risikostyringsarbejdet. Her kan der være en tendens til at vurdere risici ud fra subjektive erfaringer, og det der fylder mest i mediebilledet, frem for strukturerede metodiske vurderinger. En løsning kunne være at opstille faste modeller og strukturer for risikovurderingsarbejdet, som fordrer transparens og faglig forankring, og som guider målgruppen igennem samme modus. Dette bidrager dermed til at reducere uhensigtsmæssig formodningsdannelse. I eksemplet kan grebet 'guide målgruppen' fra nedenstående altså finde anvendelse.

Hvis det identificerede adfærdsproblem omhandler formodningsdannelse, kan følgende greb overvejes:

Afsendereffekt

Mennesker bliver i høj grad påvirket af, hvem der er afsender på et givet budskab, og vurderer sandfærdigheden eller sandsynligheden af et budskab ud fra, hvordan de opfatter afsenderens troværdighed. Det kan bruges som et aktivt greb til at opnå en ønsket adfærd. Det bør således overvejes, hvem der er afsender i en adfærdsindsats. Det kan være hensigtsmæssigt at dele målgruppen op i undergrupper, der modtager det samme budskab, men fra forskellige afsendere, eksempelvis it-chefen, den administrerende direktør, nærmeste fagleder eller juridiske afdeling.

Guide målgruppen

For at imødekomme de mentale genveje, som mennesker er tilbøjelige til at vælge, kan det hjælpe at opstille modeller, der skitserer konsekvenser af forskellige valg for at give følelsen af overblik for målgruppen. Et greb kan være et beslutningstræ, der dels skaber overblik over mulige valg for målgruppen, og dels viser resultatet af forskellige veje, målgruppen kan vælge. Det kan eksempelvis være et beslutningstræ angående sikker anskaffelse af specialsoftware, hvor kriterier og muligheder klart skitseres.

Fremhæv hvad andre gør

Mennesker er sociale væsener, og viden om sociale identiteter og fællesskaber kan bidrage til en ønsket adfærd. Særligt i situationer med stor grad af usikkerhed, vil folk ofte kigge mod andre med den formodning, at de andre ved, hvad der sker, og derfor handler 'rigtigt' i den givne situation. Grundlæggende vil mennesker gerne gøre det samme som flertallet. Fremhævning af, at andre udfører den ønskede adfærd, kan

derfor bruges som et greb til at påvirke den uønskede adfærd. Det kan eksempelvis være information om, hvor mange medarbejdere, der allerede har gennemført et obligatorisk it-kursus.

Problem: Valg

Hvis analysefasen har vist, at det aktuelle adfærdsproblem skyldes den måde, der træffes valg på, kan der arbejdes på en adfærdsindsats, der gør det ønskede valg attraktivt. Når mennesker står over for et valg, så vælger de det, de opfatter som det mest attraktive. Et valg foretages ikke alene på baggrund af rationelle overvejelser. Faktisk er følelser en fundamental faktor, når der træffes valg. Ved et valg simuleres konsekvenserne af at vælge en mulighed frem for en anden, og det aktiverer automatisk en følelsesmæssig respons.

Et eksempel herpå er brug af usikre trådløse netværk på rejser. Tanken om eventuelt at løbe tør for mobildata kan medføre, at der anvendes et usikkert trådløst netværk uagtet risici og faktiske behov for mobildata. Et valg, der kan forsøges påvirket ved at tilbyde fri data på eksempelvis tjenesterejser. At planlægge ud fra at aktivere følelser kan derfor anvendes til at gøre kedelige, men fordelagtige valg mere attraktive.

Handler adfærdsproblemet om uhensigtsmæssige valg, kan adfærdsindsatsen påvirke valgprocessen ved at gøre brug af nedenstående greb:

Framing

Når mennesker står over for en række valgmuligheder, står de samtidig over for en række mulige fremtider. Framing handler om at præsentere den samme information, hvor nogle aspekter af situationen og de potentielle fremtidige konsekvenser fremhæves, mens andre nedtones. Formålet er, at én mulighed vælges over en anden på grund af måden, mulighederne præsenteres eller formuleres på.

Kompromis-effekten

Kompromis-effekten beskriver den menneskelige tendens til at fravælge 'ekstremerne' og vælge en løsning, der placerer sig i midten. Det kan bruges aktivt i en adfærdsindsats. Præsenterer man eksempelvis tre niveauer; god (niveau 1), bedre (niveau 2), bedst (niveau 3) for sikker håndtering af dokumenter, vil flere vælge bedre (niveau 2), end hvis valget alene stod imellem god (niveau 1) og bedst (niveau 2).

Problem: Vedholdenhed

Hvis analysefasen har vist, at det aktuelle adfærdsproblem skyldes manglende vedholdenhed, kan der arbejdes på en adfærdsindsats, der gør det nemt at fastholde den ønskede adfærd over tid. Det er nemt at have et ønske om at gøre noget. Det bliver først svært, når det skal gøres. Det er dog ikke altid, at mennesker forventer, at det vil blive svært. Der ses en systematisk menneskelig tendens til at overvurdere egne evner til at gøre det, der kræves for at nå det ønskede. Det at vælge at gøre noget, er derfor ikke det samme som, at det lykkedes. Eksempelvis kan en organisation have ønske om, at medarbejderne systematisk indrapporterer formodede phishing e-mails. Det sker dog kun sporadisk og hypotesen er, at det skyldes mang-

lende feedback, når en medarbejder rapporterer en mistænkelig mail, eller at medarbejderne har en oplevelse af, at det er besværligt og tidskrævende at indrapportere formodede phishing e-mails.

Er den ønskede adfærd opnået i første omgang, men problemet er analyseret til at være manglende vedholdenhed af den ønskede adfærd, kan følgende greb inkluderes i adfærdsindsatsen:

Øg eller formindske barrierer

En ønsket adfærd kan fremmes ved at mindske barriererne for handlingen, ligesom en barriere kan vanskeliggøre den uønskede adfærd. Barrieren kan eksempelvis mindskes ved at reducere antallet af klik, som en ønsket handling kræver i et system. Grundlæggende handler det om at gøre den ønskede adfærd relativt nemmere sammenlignet med den uønskede adfærd.

Handleplaner

Udarbejdelse af konkrete og specifikke handleplaner er et greb til at fastholde en ønsket adfærd. Planerne beskriver en kontekstspecifik fremgangsmåde til at nå målet ud fra devisen: "hvis X sker, så handler jeg efter plan A". Eksempelvis beredskabs-handleplaner. De forskellige handleplaner beskriver, hvordan et specifikt scenarie skal håndteres. Mennesker er mere tilbøjelige til at have en bestemt adfærd, hvis de har en plan for hvordan, hvornår og hvor de skal udføre handlingen.

Sådanne handlingsplaner skaber mentale repræsentationer af fremtidige situationer, hvilket sandsynliggør, at planen automatisk aktiveres. Hvis handlingerne gentages, vil de over tid blive en rutine eller vane, der ikke kræver bevidste valg og handlinger.

Systematisk feedback

Feedback bidrager også til at fastholde en adfærd over tid. Hvis der gives systematisk feedback om status og fremskridt, er der større sandsynlighed for at nå et fastsat mål, som for eksempel en ønsket adfærd. Feedback kan eksempelvis være real-time feedback, som teknisk eller automatisk feedback, eksempelvis efter rapportering af en phishing e-mail. Endelig kan det også være mundtlig eller skriftlig feedback fra chef eller kolleger.

Forpligtelser (sociale eller faglige)

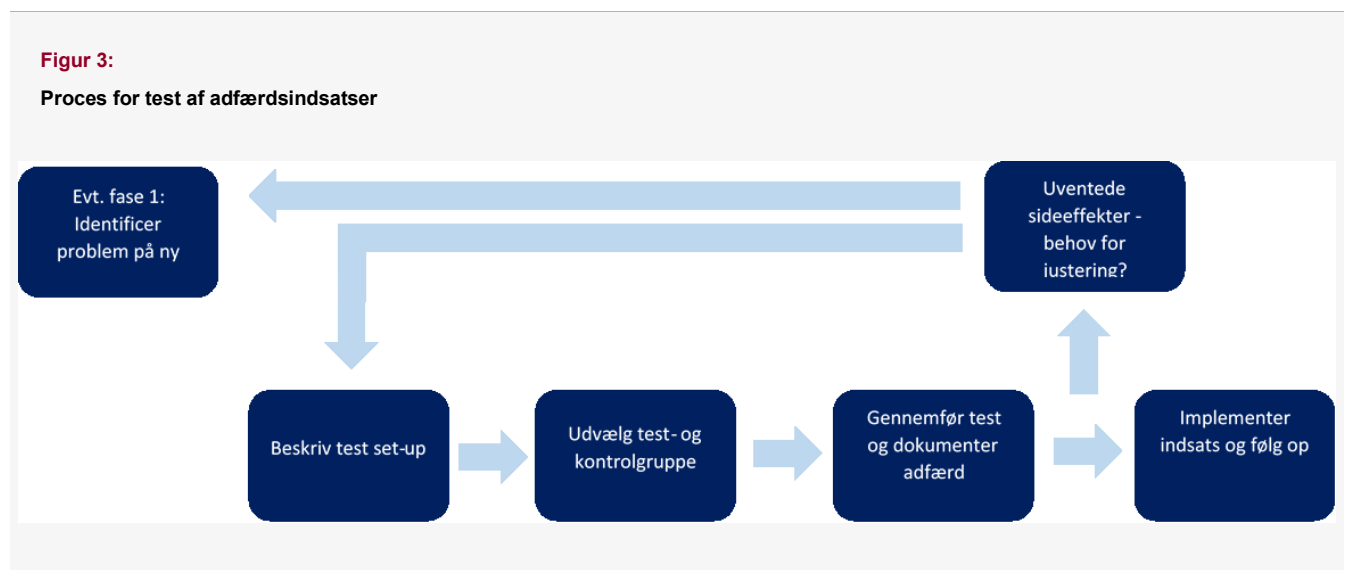
Hvis mennesker aktivt forpligter sig til at gennemføre en bestemt adfærd overfor blandt andet kolleger eller samarbejdspartnere er de mere tilbøjelige til at leve op til deres gode hensigter, end hvis målet ikke formuleres "offentligt".

Fase 4: Test adfærdsindsatsen

Når adfærdsindsatsen er udarbejdet med brug af ovenstående greb, skal den testes, hvilket sker i testfasen. Det primære formål er at afprøve, om den valgte adfærdsind-

sats bidrager til den ønskede adfærd. Desuden skal testfasen bidrage til at klarlægge, om adfærdsindsatsen medfører uventede 'sideeffekter', positive eller negative.

Den planlagte adfærdsindsats testes i mindre skala, inden den eventuelt implementeres fuldt ud. På den måde kan erfaringer inddrages, og adfærdsindsatsen kan eventuelt tilpasses. Nedenfor præsenteres en praktisk tilgang til at teste en adfærdsindsats, efterfulgt af en mere kvalitativ undersøgelse af eventuelle sideeffekter.



1. Beskriv test-setup, herunder testperiode og SMART-målsætning inklusiv succeskriterie, som eksempelvis kan være, at en vis procentdel af testgruppen udfører den ønskede handling.

2. Herefter begynder udvælgelsen af testdeltagere. Deltagerne bør være en undergruppe af målgruppen for den pågældende adfærdsindsats. Udvalgte testdeltagere til at teste adfærdsindsatsen, skal deltagerne fordeles i en testgruppe og i en kontrolgruppe. Det bør være tilfældigt, hvem der deltager i henholdsvis den ene og den anden gruppe. Det er for, ideelt set, at sikre, at den eneste forskel mellem de to grupper er adfærdsindsatsen. I praksis er det dog oftest ikke muligt at gennemføre en test, hvor det er den eneste forskel. Testen kan dog stadig bidrage til at undersøge adfærdsindsatsens brugbarhed.

3. Begynd testen og dokumenter adfærden på de to variabler (adfærdsindsats, mål) i begge grupper. Testgruppen vil udsættes for adfærdsindsatsen, mens kontrolgruppen ikke udsættes for adfærdsindsatsen. De to gruppers testresultater analyseres for at se, om der er forskelle i gruppernes adfærd. Eksempelvis om den ønskede adfærd optræder hyppigere hos testgruppen end hos kontrolgruppen, og om det i så fald er tilstrækkeligt til at opfylde det opstillede succeskriterie. Hvis det er tilfældet, er næste

skridt at planlægge den fulde implementering af adfærdsindsatsen. Inden da bør det undersøges, om adfærdsindsatsen medfører uventede sideeffekter.

4. I den første test ved man, hvad man kigger efter og måler på: Fører adfærdsindsats X til ønsket adfærd Y. Når man skal teste for eventuelle sideeffekter, bliver det straks vanskeligere, fordi man ikke ved, hvad man præcist leder efter. Viser den første test, at adfærdsindsatsen synes at virke, er det dog værd at udvide blikket og være åben for eventuelle sideeffekter. Det kan gøres på flere måder afhængig af kontekst og ressourcer. Mulige metoder kan være 1) observation af test- og kontrolgruppe, mens de udsættes for adfærdsindsats / status quo, og 2) spørgeskema med åbne spørgsmål, der sendes ud efter adfærdsindsats for at få en øget indsigt i, hvordan de to grupper oplevede adfærdsindsatsen / status quo. Her er det vigtigt at holde sig for øje, at positiv respons ikke kan tages som succes, hvis der ikke observeres en reel adfærdseffekt.

I analysen af testresultaterne kan det vise sig, at den pågældende adfærdsindsats har uventede sideeffekter, der som nævnt kan være såvel positive som negative. Det kan betyde, at adfærdsindsatsen skal tilpasses den nye viden og derefter testes igen. Det kan også vise sig, at adfærdsindsatsen ikke har effekt på den ønskede adfærd, men at den i stedet virker på en anden adfærd. I så fald bør man identificere, om det drejer sig om et adfærdsproblem jf. fase 1, som man ønsker at ændre og i så fald gennemgå faserne igen. Testen er en god anledning til at genbesøge SMART-målsætningen for at sikre sig, at adfærdsindsatsen stadig er på ret spor, og at målsætningen er realiserbar.

Det skal også løbende samt i testfasen overvejes, om adfærdsindsatsen har nogle sideeffekter, hvor man risikerer at komme på kant med etiske eller juridiske grænser for, hvad man kan eller bør gøre.

Testresultaterne bør forelægges ledelsen, og der bør sikres godkendelse herfra, inden implementeringen af adfærdsindsatsen igangsættes. På den måde sikres det, at der er grønt lys til eksempelvis at inddrage andre afdelinger i implementeringsarbejdet, til at systemer eller processer ændres, eller til at allokere yderligere ressourcer til arbejdet.

Fase 5: Implementer adfærdsindsatsen og følg op

I fase 5 skal adfærdsindsatsen implementeres i fuld skala. Formålet med denne sidste fase er at implementere adfærdsindsatsen og fastholde den ønskede adfærd over tid. Der bør udarbejdes en implementeringsplan, der også inkluderer en plan for monitorering og evaluering af den ønskede adfærd og eventuelle sideeffekter. Ændringer af adfærd kan tage tid, og det vil variere, hvor hurtigt den ønskede adfærd opnås. I nogle tilfælde kan der ske en ændring af adfærden med det samme, men over tid kan adfærden ændre sig igen. Enten tilbage til den uønskede adfærd eller til

noget uforudset, som ikke kom frem under testfasen. Monitorering kan gennemføres med de nævnte metoder i testfasen.

I denne sidste fase vil det også være relevant at holde den implementerede indsats og dens sideeffekter op mod SMART-målsætningen for at vurdere, hvor indsatsen lykkedes og ikke lykkedes, og hvor fremtidige indsatser vil kunne justeres og forbedres. I denne vurdering af effekt kan SMART-målsætningen holdes op mod den uhenigtsmæssige adfærd, som først blev identificeret. Effektmålingen kan være et godt redskab for ledelsen til at vurdere prioritering af midler samt fremtidige indsatsområder.

Når adfærdsindsatsen skaleres, er det vigtigt at holde sig for øje, at testens resultater knytter sig til den specifikke situation og målgruppe. De kan derfor ikke umiddelbart generaliseres til at virke på alle personer i alle situationer. Det er derfor heller ikke anbefalelsesværdigt at blindt kopiere en vellykket adfærdsindsats fra tidligere, eller fra en lignende organisation for at spare analyse- og testfasen væk. Et grundlæggende princip for at lykkes med en adfærdsindsats er netop, at den er baseret på data om den konkrete uønskede adfærd med henblik på at forstå, hvorfor medarbejderne gør, som de gør. Det anbefales derfor altid at gennemføre en test af den konkrete adfærdsindsats på de pågældende medarbejdere i den aktuelle kontekst.

3. Afrunding

Metoden bidrager til en forståelse for, hvorfor mennesker agerer, som de gør, og giver en metode til, hvordan den viden aktivt kan anvendes i arbejdet med informationssikkerhed. I Bilag 1 præsenteres en case, hvor metoden gennemgås.

4. Referencer

90% of UK Data Breaches Due to Human Error in 2019, Infosecurity Magazine, <https://www.infosecurity-magazine.com/news/90-data-breaches-human-error/>

A Handbook of Media and Communication Research: Qualitative and Quantitative Methodologies, Klaus Bruhn Jensen, Routledge, 2012

At tænke – hurtigt og langsomt, Daniel Kahneman, dansk udgave, Lindhardt og Ringhof, 2018

Datatilsynets statistikbank over fordeling af hændelser, Datatilsynet, <https://www.datatilsynet.dk/sikkerhedsbrud/statistik-over-anmeldte-sikkerhedsbrud>

Human error is still the number one cause of most data breaches in 2021, Influence, <https://www.influencive.com/human-error-is-still-the-number-one-cause-of-most-data-breaches-in-2021/>

IBM X-Force Threat Intelligence Index 2017 & 2018, IBM

Kodeks for gennemførelse af sikkerhedstests 2021, Center for Cybersikkerhed, Digitaliseringsstyrelsen, KL m.fl., https://digst.dk/media/23689/kodeks_for_sikkerhedstest_2021_digst.pdf

Metoder i statskundskab, redigeret af Lotte Bøgh Andersen, Kasper Møller Hansen, Robert Klemmensen, Gyldendal, 2010

The Definition of Nudge and Libertarian Paternalism: Does the Hand Fit the Glove?, Pelle Guldborg Hansen i: *European Journal of Risk Regulation*, 2016

Tools and Ethics for Applied Behavioural Insights: The BASIC Toolkit, OECD Publishing, Paris, <https://doi.org/10.1787/9ea76a8f-en>, OECD, 2019

5. Bilag

Case: Adfærdsproblem med ulåste pc'er

Fase 1: Identificer problemet og sæt mål for ønsket adfærd

En organisation, der håndterer både persondata og sensitive dokumenter, har et problem med ulåste pc'er, når medarbejderne forlader deres kontorplads i løbet af arbejdsdagen. Eksterne konsulenter, samarbejdspartnere og kunder færdes jævnligt og frit i organisationen. En nyligt gennemført undersøgelse viser, at alle medarbejdere ved, at de skal låse deres pc, og forstår hvorfor. Da it-sikkerhedsafdelingen gennemgår de tomme kontorer i frokostpausen hver dag i en uge, viser det sig alligevel, at 60 procent af pc'erne ikke er låst. Dog skiller HR-afdelingen sig ud, da der her kun er to procent af pc'erne, der ikke er låst. HR-afdelingen har længe haft et øget fokus på håndtering af persondata, hvilket kan forklare den anderledes adfærd.

Der er tradition for, at alle går til frokostpause kl. 11.30, hvor kantinen åbner. Da frokostpausen er det eneste tidspunkt i løbet af en arbejdsdag, hvor stort set alle medarbejdere går fra deres kontorplads samtidigt, begrænses adfærdsproblemet i nærværende indsats til at omhandle netop det tidspunkt.

Fase 2: Analyser og diagnosticer adfærdsproblemet

Hypotese

Medarbejderne glemmer at låse deres pc grundet højt arbejdspress.

Dataindsamling

Data viser, at antallet af sendte og modtagne mails og antal møder – interne og eksterne – er langt størst i tidsrummet 9.00 – 11.30, hvilket kan indikere et øget arbejdspress i netop det tidsrum.

Observation

Målgruppen observeres fra kl. 11.15 og til alle er gået til frokost. Desuden observeres kantinen i tidsrummet fra 11.20 -13.00

Indsigt: Alle går til frokost inden for et interval på tre minutter.

Indsigt: I kantinen observeres, at der er lang kø, og buffeten bliver hurtig halvtom og fyldes ikke op igen.

Konklusion

Medarbejderne låser ikke deres pc'er, da de op til frokost har øget arbejdspress og dermed opmærksomhed på igangværende opgaver, og/eller fordi de føler, at de skal skynde sig til kantinen, inden maden er væk.

Fase 3: Udarbejd adfærdsindsatsen

Med afsæt i analysen udvælges greb, der forventes at bidrage til den ønskede effekt. Da analysen viser, at det primære problem er manglende opmærksomhed, udvælges

to greb, der skal drage medarbejderes opmærksomhed hen på at låse pc'en inden de går til frokost, plus en ændring i konteksten, der ligeledes kan bidrage til den ønskede adfærd.

- Trafikdata fra intranettet viser, at cirka 90 procent af alle medarbejderne tjekker dagens frokostmenu på intranettet i løbet af formiddagen. På menuen indsættes derfor en tekst, hvor der står: Lås venligst din pc, når du går til frokost.
- Pop-up besked på alle medarbejderes pc'er kl. 11.20, der minder om, at folk skal låse deres pc ved hjælp af genvejstasten \square + L, når de går til frokost.
- Kontekst betyder meget for folks handlinger. Analysefasen viste, at mange medarbejdere føler, at de skal skynde sig til frokost kl. 11.30, da der hurtigt bliver kø til buffeten ligesom, at udvalget hurtigt reduceres. En del af indsatsen er derfor en aftale med køkkenpersonalet, der dels udvider frokostpausen med 30 minutter og dels fylder buffeten op igen kl. 12.15.

Fase 4: Test adfærdsindsatsen

1. Test-set-up

Testgruppen modtager menu med tekst, pop-up med påmindelse samt information om udvidet åbningstid + ekstra opfyldning. Ideelt set bør hver indsats testes separat med henblik på at vise, om og i så fald, hvilket greb i indsats der bidrager til den ønskede adfærd. Afhængig af ressourcer, kan hele indsatsen dog testes samlet.

Hos kontrolgruppen er der ingen indsats. Det vil sige, at de modtager den sædvanlige menu, ingen pop-up med påmindelse, og de får ikke information om kantinens udvidede åbningstid.

2. Test- og kontrolgruppe

Testgruppen: Seks medarbejdere; tre tilfældigt udvalgt fra kommunikationsafdelingen og tre tilfældigt udvalgt fra udviklingsafdelingen.

Kontrolgruppe: Seks medarbejdere; tre tilfældigt udvalgt fra kommunikationsafdelingen og tre tilfældigt udvalgt fra udviklingsafdelingen.

Testen gennemføres i uge 16 og adfærd dokumenteres ved at tjekke de to gruppers pc'er umiddelbart efter, at de er gået til frokost.

Succeskriterie: At reducere antallet af ulåste pc'er fra 60 procent til 20 procent blandt målgruppen (alle medarbejdere, minus HR-afdelingen)

3. Testen gennemføres og adfærd dokumenteres

Resultat af testen: Indsatsen synes at bidrage til den ønskede adfærd: låste pc'er, når medarbejdere går til frokost. I testgruppen låser 85 procent af medarbejderne deres pc, inden de går til frokost, mens der i kontrolgruppen fortsat kun er 40 procent, der låser deres pc. Det opstillede succeskriterie nås således i testen.

Fase 5: Implementer adfærdsindsatsen og følg op

Implementeringsplan

Uge 18:

Indsatsen implementeres i hele organisationen. Der kommunikeres også om ændringerne i kantinen.

Uge 24, 36 og 44:

Indsatsen monitoreres med det formål at undersøge, om den ønskede adfærd er bibeholdt, eller om der er behov for at ændre indsatsindsatsen. Monitoreringen foregår dels ved at undersøge, om pc'erne er låst, når medarbejderne går til frokost, og dels ved on-the-spot interviews, hvor medarbejdes spørges om, hvorfor de har låst eller ikke låst deres pc.

Sideeffekter

Uge 24 og 44 afholdes der fokusgrupper, hvor eventuelle sideeffekter drøftes. Kantine fortæller, at de oplever mindre madspild, nu hvor de fylder buffeten op to gange efter behov. Flere medarbejdere oplever mindre stressende formiddage, da de ikke skal skynde sig til frokost på et bestemt tidspunkt. Få medarbejdere irriteres over den tilbagevendende pop-up-besked, der nærmest giver dem lyst til at trodse beskeden og efterlade pc'en ulåst.

I uge 36 gennemføres desuden observationer i udvalgte afdelinger for at undersøge, om den opnåede adfærd med at låse pc'er i frokostpausen har haft en affledt effekt på låsning af pc'er, når arbejdspladsen forlades af andre grunde, eksempelvis møder eller toiletbesøg. Stikprøverne viser, at den uønskede adfærd i de tilfælde er 30 procent, hvilket formodes at være på grund af indsatsen.



Metode til at arbejde med adfærdsindsatser inden for cyber- og informationssikkerhed

Udgivet juli 2021

Udgivet af Center for Cybersikkerhed og Digitaliseringsstyrelsen

Publikationen er kun udgivet elektronisk

Henvendelse om publikationen kan i øvrigt ske til:

Center for Cybersikkerhed
Kastellet 30
2100 København Ø
Tlf. 33 32 55 80

Digitaliseringsstyrelsen
Landgreven 4
1017 København K
Tlf. 33 92 52 00

Publikationen kan hentes på:

www.sikkerdigital.dk og www.cfcs.dk

Foto: Colourbox

ISBN 978-87-93073-38-8