ERHVERVSSTYRELSEN

KRAVSPECIFIKATION

”Udvikling og udbredelse af et sikkerhedstjek”

28. september 2015
Sagsnr.

1. Indledning

1.1 Formål med opgaven, der udbydes

Erhvervsstyrelsen igangsætter et arbejde med at udvikle et online sikkerhedstjek, primært rettet mod små og mellemstore virksomheder. Det skal ske med afsæt i konceptet Sikkerhed i Balance (SIB), der er en række aktørers (bl.a. Rådet for digital Sikkerhed) bud på, hvordan virksomheder kan opnå det rette IT-sikkerhedsniveau med udgangspunkt i en kategorisering af virksomhedstyper og risikoprofiler.

Derfor ønsker Erhvervsstyrelsen at udbyde opgaven med udviklingen af et sikkerhedstjek, herunder færdigudvikling af selve spørgerammen, vejledningsmateriale, konkrete værktøjer til fremme af IT-sikkerheden i virksomhederne samt en kommunikationsplan for udbredelse af værktøjet.

Udarbejdelsen af den digitale platform, hvor Sikkerhedstjekket skal ligge, indgår *ikke* i nærværende udbud.

1.2 Baggrund for opgaven

Der blev indgået en bred politisk aftale den 26. februar 2015 om Vækstplan for digitalisering i Danmark. Det følger bl.a. af vækstplanen, at IT- og datasikkerheden i dansk erhvervsliv skal styrkes for at imødegå et nyt og voksende trusselsbillede. Erhvervsstyrelsen har til opgave i samarbejde med relevante aktører at udvikle et risikobaseret sikkerhedstjek, som skal bistå virksomhederne, herunder særligt små og mellemstore virksomheder (SMV'er), med at leve op til centrale tekniske og informationsmæssige sikkerhedskrav. Sikkerhedstjekket skal bygge på eksisterende internationale standarder og tage afsæt i informationssikkerhedsstandarden ISO27001.

Rådet for Digital Sikkerhed og Erhvervsstyrelsen er gået sammen om at lave et sikkerhedstjek.

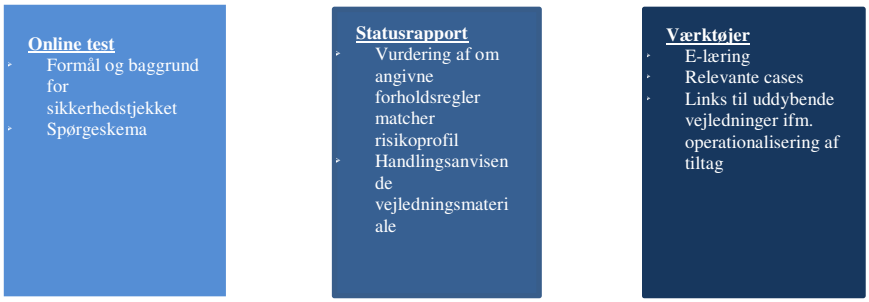
1.3 Overordnet koncept

Sikkerhedstjekket skal være et online værktøj, der med afsæt virksomhedens besvarelse af et spørgeskema skal give et risikobaseret statusbillede af virksomhedens informationssikkerhed. På baggrund heraf skal virksomheden modtage handlingsanvisende vejledningsmateriale, der skal fremme virksomhedernes informationssikkerhed.

Online test

Virksomhederne udfylder en række spørgsmål til brug for vurderingen af virksomhedernes risikoprofil og nuværende niveau af informationssikkerhed, jf. figur 1.

Figur 1: Faserne i et IT-sikkerhedstjek



Statusrapport

På baggrund af virksomhedernes svar genereres en statusrapport, som rummer en vurdering af virksomhedens risikoprofil og på baggrund heraf angiver forslag til målrettet handlingsanvisende information og vejledning, der skal fremme virksomhedens informationssikkerhed.

Værktøjer

Virksomheden præsenteres for uddybende handlingsanvisende informations- og vejledningsmateriale, relevante inspirationscases, e-læringsmateriale, eksemplificerende videofilm og evt. også henvisninger til, hvor virksomheden kan få yderligere inspiration og rådgivning.

Til inspiration kan der tages afsæt i, hvorledes fx UK, Norge og USA arbejder med at fremme informationssikkerheden i erhvervslivet – særligt SMV:

I UK har man udviklet et tjek, der primært har fokus på de internettekniske elementer af sikkerheden – fx om virksomheden har en firewall.
https://www.iasme.co.uk/index.php/cyberessentialsprofile

Det norske sikkerhedstjek, der har afsæt i ISO27001, findes her:
https://sikkerhetssjekk.norsis.no/

I USA har Security Industry and Financial Markets Association (SIFMA) har udviklet et værktøj rettet mod SMV-segmentet:

http://www.sifma.org/issues/operations-and-technology/cybersecurity/guidance-for-small-firms/

Der er også en række danske aktører inden for feltet, der laver informations- og vejledningsmateriale rettet mod målgruppen:

DI ITEK har bl.a. lavet en række vejledninger om privacy og informationssikkerhed – herunder også nogle rettet mod SMV.

http://itek.di.dk/viden/vejledninger/Pages/Vejledninger.aspx

Ligeledes har Digitaliseringsstyrelsen udarbejdet vejledningsmateriale fx guide til forenklet implementering af ISO27001 og vejledning indeholdende en prioriteret køreplan henvendt til ledelsesniveauet i offentlige myndigheder og private virksomhed for, hvordan risikoen for cyberangreb kan mindskes:

http://www.digst.dk/Servicemenu/Nyheder/Nyhedsarkiv/Digitaliseringsstyrelsen/2013/cyberforsvar

1.4 Opgavebeskrivelse

I forbindelse med udvikling af et dansk sikkerhedstjek er der således som skitseret under det overordnede koncept en række opgaveelementer, der skal løftes.

1. Konceptdesign
2. Online spørgsmål bag Sikkerhedstjekset og brugertest
3. Handlingsanvisende vejledningsmateriale – statusrapport og værktøjer
4. Plan for udbredelse af tjekket.

Udviklingen af den digitale platform og den underlæggende arkitektur, der skal gøre det muligt for virksomhederne på baggrund af spørgsmålsbesvarelser at modtage relevant vejledning er ikke en del af nærværende udbud. Den udarbejdes af eksterne konsulenter for Rådet for Digital Sikkerhed. Der forventes løbende dialog mellem vinderen af nærværende udbud og Erhvervsstyrelsen/Rådet for Digital Sikkerhed om de tekniske rammer, som værktøjet skal fungere indenfor.

1. Konceptdesign

Der ønskes et bud på et sammenhængende konceptdesign fra online spørgsmål til vejledningsmateriale og udbredelse af tjekket. Konceptdesignet skal have fokus på at

sikre et brugervenligt og effektivt flow for virksomhederne fra besvarelse af spørgsmål til vejledningsmaterialet. Særlig opmærksomhed skal der være på at sikre, at spørgsmål/svar i spørgeskemaet matcher vejledningsmaterialet og dermed tager afsæt i en risikobaseret statusrapport. Målgruppen for værktøjet er SMV'er. Rådet for Digital Sikkerhed har allerede udviklet en første prototype på værktøjet – og tilhørende spørgeramme.

2. Online spørgsmål bag sikkerhedstjek og brugertest

I den eksisterende prototype er der allerede formuleret et første bud på spørgsmål af Rådet for Digital Sikkerhed. Disse spørgsmål skal brugertestes på målgruppen – SMV'erne. Spørgsmålene skal kortlægge den enkelte virksomheds risikoprofil og tilhørende behov for indsats. Det skal tilsigtes, at det er ledelsen (evt. med bistand fra den IT-ansvarlige) i virksomheden, der skal svare på de endelige spørgsmål. Spørgsmålene skal være letforståelige, og der skal kunne svares ja/nej til hovedparten af spørgsmålene. Det kan overvejes, om der til udvalgte spørgsmål er behov for foruddefinerede kategorier. Spørgsmålene skal tage afsæt i ISO27001-tilgangen, og de skal derfor ikke alene have en teknisk karakter, men også favne kategorier som organisation, processer og ledelse. Antallet og kompleksiteten af spørgsmålene skal tilpasses målgruppen, som er SMV'er med særligt fokus på virksomheder med op til 50 ansatte.

Derudover ønskes der en brugertest af spørgerammen, konceptet, flowet og opbygningen, som det ser ud nu. Spørgerammen tilpasses på baggrund heraf. Der skal samtidig testes for, hvilket behov brugerne har ift. det vejledningsmateriale, der skal udarbejdes i forlængelse af spørgerammen. Endelig skal det i forbindelse med brugertest undersøges, hvilke kanaler målgruppen ser som oplagte at udbrede tjekket via (herunder fx Virk.dk, erhvervsorganisationer, væksthuse mv.). Resultaterne heraf skal indgå i det videre arbejde. Der skal brugertestes på min 5-7 virksomheder fra målgruppen – SMV'er. ERST deltager i halvdelen af disse brugertests.

3. Handlingsanvisende vejledningsmateriale, statusrapport og værktøjer

Når virksomhederne har besvaret spørgsmålene, skal de modtage statusrapporten, der viser et statusbillede af virksomhedens informationssikkerhedsmæssige sårbarheder, det trusselsbillede virksomheden står overfor, og hvor virksomheden bør sætte ind sikkerhedsmæssigt. Formålet med rapporten er at synliggøre de informationssikkerhedsmæssige risici, som virksomheden står overfor. Der skal udarbejdes et set-up for en statusrapport med afsæt i det koncept, der allerede ligger i

SIB, hvor spørgsmål og vejledningsmateriale matches. Det forventes, at virksomhederne præsenteres for et udvalgt og målrettet udsnit af det tilgængelige vejledningsmateriale på baggrund af deres risikoprofil. Dette skal præsenteres på en overskuelig og letforståelig måde med korte introtekster/appetitvækkere til materialet, hvorfra der kan klikkes videre til det uddybende materiale.

Med afsæt i spørgsmål og det mere kortfattede vejledningsmateriale, der er beskrevet ovenfor, skal der udvikles uddybende og handlingsanvisende værktøjer.

Der skal udvikles vejledningsmateriale, der indeholder konkret inspiration til handling. Der skal indgå forskellige virkemidler i materialet – fx korte videoer, tekst, relevante links eller e-læringsforløb. Der forventes inspirerende videobaserede casebeskrivelser, der illustrerer hvordan virksomheder arbejder med informationssikkerhed, eksempler på hændelser (brud på sikkerheden) følgende konsekvenser, udfordringer, løsninger og konkurrencemæssige potentiale ved at have styr på informationssikkerheden. Der skal udvikles min. 6-8 videobaserede cases (på ca 3 min) med tilhørende faktabaseret formidlende tekst (3-5 sider).

Det er væsentligt, at statusrapport og vejledningsmateriale udarbejdes således, at det fremmer virksomhedernes incitamenter og evne til at handle på sikkerhedsudfordringerne. Materialet skal dels henvende sig til ledelsen, dels til medarbejderne i organisationen.

For vejledningsmaterialet gælder, at det skal kunne gøres tilgængeligt online, og derfor i en form, der skal tilpasses web-setup bag tjekket. Vejledningsmaterialet skal udvikles og prioriteres med afsæt i, hvad der findes af eksisterende materiale, som der evt. kan henvises til som del af materialet. Materialet skal leveres i et format der kan arbejde sammen med den digitale platform for værktøjet, der udvikles sideløbende. Dette format aftales i samarbejde med ERST, RDS samt leverandøren af den digitale platform.

4. Udbredelse af sikkerhedstjekket

Udbredelsen af kendskabet til og anvendelsen af sikkerhedstjekket forventes bl.a. fremmet via forskellige aktører, der løbende er i kontakt med målgruppen. Der skal udarbejdes en *kommunikationsplan* til brug for denne udbredelse, herunder metoder, udbredelseskanaler og aktører.

Der skal udarbejdes *informationsmateriale om sikkerhedstjek*, der kan anvendes af fx erhvervsfremmeaktører i forbindelse med deres dialog med virksomheder om IT-sikkerhed.

1.5 Metode

I forhold til opgaveløsningen forventes det, at der foretages en grundig desk research omkring mulige former for set-up af et online sikkerhedstjek, og i særdeleshed ift., hvad der allerede eksisterer af bl.a. vejledningsmateriale, der kan danne afsæt for arbejdet. Så vidt muligt bør der også hentes inspiration og sparring hos de udenlandske myndigheder, der har udarbejdet lignende tjek for at indhente erfaringer.

Det forventes, at der bliver gennemført en solid brugertest blandt virksomheder på tværs af brancher af spørgerammen og set-up, der sikrer et godt og brugervenligt sikkerhedstjek samt af forhold, der vil være afgørende for at nå ud til målgruppen, at målgruppen finder værdi i værktøjet og faktisk tager det i brug.

Der ønskes et forslag til en proces for, hvordan relevante aktører kan blive inddraget på centrale tidspunkter i forløbet.

1.6 Tilbudsmaterialet skal indeholde

Tilbudsgiver bedes give bud på, hvordan opgaven vil blive løftet, og tilbudsmaterialet skal som minimum indeholde:

- Beskrivelse af tilbudsgivers bud på det overordnede koncept med online spørgsmålskategorier, vejledningsmateriale og udbredelse, der vurderes at give størst effekt hos målgruppen.
- Tilbudsgivers bud på, hvordan der tænkes brugertestet og tilpasset spørgsmål til sikkerhedstjekket, som er anvendeligt og skaber effekt hos målgruppen.
- Overordnet bud på, hvilken type vejledningsmateriale som tilbudsgiver vurderer væsentlig at udvikle og stille til rådighed for målgruppen, herunder også en beskrivelse af hvilke typer af supplerende værktøjer (fx e-læring, brug af videocases, etc.) tilbudsgiver finder relevant.
- Bud på, hvordan forskellige aktører - fx erhvervsfremmeaktører, revisorer - kan inddrages og støttes i at rådgive virksomheder til at tage tjekket, samt inddrages i udvikling af konceptet.
- Tidsplan med indlagte delleverancer og slutleverance.

- Budget med angivelse af de vigtigste budgetposter.
- Samlet pris for at udføre opgaven.
- Beskrivelser af tilbudsgivers erfaring med frembringelse vejledningsmateriale herunder fx audiovisuelt og tekstligt materiale – kendskab til informationssikkerhed og ISO27001, erfaring med vejledning af mindre virksomheder omkring informationssikkerhed - herunder de allokerede medarbejderes kompetencer og erfaringer

Tilbudsgiver vil få ansvaret for alle opgaver, men der skal påregnes et tæt samarbejde med ERST under hele forløbet. ERST skal godkende delleverancer, inden næste delleverance igangsættes.

1.7 Kriterier for valg af tilbud

I det samlede tilbud fra konsulentvirksomheden vil der blive lagt vægt på:

- Samlede forslag til undersøgelsesdesign og opgaveforståelse
- Tilbudsgivers erfaring med at kommunikere til målgruppen
- Bemanding og disses kompetencer
- Pris
- Tidsplan

Det er væsentligt, at den samlede bemandingsmæssige sammensætning kan påvise følgende kompetencer:

- Kendskab til informationssikkerhed, herunder ISO27001-baserede tiltag
- Erfaring med udvikling af vejledningsmaterialer såsom videocases, skriftlige vejledningsmaterialer mv. Dokumenteret forståelse for og erfaring med kommunikation og andre tiltag rettet mod SMV'er.

1.8 Samarbejde med Erhvervsstyrelsen

Erhvervsstyrelsen skal løbende inddrages i gennemførelsen af opgaveløsningen, bl.a. i form af løbende møder, hvor fremdriften og status på opgaveløsningen præsenteres og drøftes. De enkelte delelementer af opgaveløsningen skal godkendes af Erhvervsstyrelsen, inden der arbejdes videre med næste opgave. Derfor
forventes som minimum et møde i forbindelse med hver delleverance (se pkt 1.4 - opgaver), hvor den konkrete leverance drøftes samt tilgang til den næste.

Der forventes en løbende dialog med Erhvervsstyrelsen omkring fremdrift og status. Endvidere forventes der 1-2 møder med styregruppen for sikkerhedstjekket, hvor status og fremdrift præsenteres.

Derudover skal delelementerne præsenteres for og drøftes med styregruppen på 1-2 møder forud for afslutningen af den endelige opgave.

1.9 Betaling

Opgaven skal gennemføres for under 1.000.000 kr. eksklusiv moms og kan evt. udbetales i rater, der følger de enkelte leverancer efter godkendelse af ERST.

1.10 Kontaktoplysninger

Følgende personer fra Erhvervsstyrelsen kan kontaktes vedrørende analyseopgaven og spørgsmål i forbindelse med udbuddet: Anna Bay Damholt: anbada@erst.dk

Alle stillede spørgsmål og svar vil blive videresendt til alle, som har tilkendegivet interesse i at give tilbud på opgaven.

2. Kravspecifikationens opbygning

2.1 Kravmetodik

De krav, som tilbudsgiver eksplicit skal besvare, fremgår af nedenstående tabeller.

Kravene ønskes besvaret i tilbuddet på en sådan måde, at det tydeligt fremgår, hvilken opgaveløsningsbeskrivelse mv., der svarer til det enkelte krav. Dette kan for eksempel ske ved, at løsningsbeskrivelsen mv. refererer til kravnumrene i tabellen nedenfor under punkt 3.

2.2 Kravtyper

Erhvervsstyrelsens krav til den udbudte opgave er nærmere beskrevet i tabellen under punkt 3. I kolonnen "Type" er kravene angivet som enten mindstekrav (MK) eller evalueringskrav (EK).

2.2.1 Mindstekrav (MK)

Mindstekrav er krav til ydelsen, som *skal* indgå som en del af den samlede ydelse.

Leverandøren skal således altid opfylde mindstekrav, og der kan ikke tages forbehold i tilbuddet for mindstekrav. Anføres det i tilbuddet, at et mindstekrav ikke vil blive opfyldt, eller der i øvrigt tages forbehold for opfyldelse af mindstekravet i tilbuddet, er Erhvervsstyrelsen forpligtet til at afvise hele tilbuddet som ukonditionsmæssigt. Tilbudsgiver indestår således for ved afgivelse af sit tilbud for, at samtlige mindstekrav kan opfyldes.

2.2.2 Evalueringskrav (EK)

Evalueringskrav er at opfatte som Erhvervsstyrelsens ønske om en bestemt egenskab eller et bestemt vilkår. Såfremt et tilbud ikke opfylder et evalueringskrav hele eller delvist, vil det blive tillagt vægt i forbindelse med den endelige evaluering. Det betyder, at det vil kunne trække ned i den samlede vurdering, såfremt et tilbud ikke eller kun i ringe grad opfylder et evalueringskrav.

2.3 Om det samlede udbudsmateriale

Dette bilag er en del af det samlede udbudsmateriale og udgør en del af aftalegrundlaget for levering af den udbudte ydelse. En oversigt over det samlede udbudsmateriale findes i udbudsbetingelserne.

Eventuelle forbehold til krav i dette bilag skal fremgå af det i udbudsbetingelserne omtalte skema over forbehold.

Interesserede tilbudsgivere opfordres til at stille spørgsmål til Erhvervsstyrelsen, jf. nærmere herom i udbudsbetingelserne, såfremt der måtte være afklarende spørgsmål til kravspecifikationen.

3. Erhvervsstyrelsens krav til leverancen

Nr.	Type	Kravtekst
01	MK	Oplæg til proces-, tids- og fremgangsmådeplan for: 1. Beskrivelse af koncept – hvordan et sammenhængende værktøj skal se ud 2. Brugertest og tilpasning og af online spørgeskema 3. Handlingsanvisende vejledningsmateriale – statusrapport og værktøjer 4. Plan for udbredelse af tjekket.
02	EK	Forslag til et klart, let forståeligt sammenhængende og selvstændigt konceptdesign, se pkt. 1.4
03	MK	Bud på hvilke elementer en brugertest skal indeholde, hvilke typer samt antal virksomheder, der skal brugertestes samt, hvorledes resultatet heraf skal føre til tilpasninger i eksisterende spørgeramme samt indgå i løsningen af de resterende opgaver. Se pkt. 1.4.
04	MK	Beskrivelse af: *hvordan statusrapporten skal udformes hvordan det handlingsanvisende vejledningsmateriale skal udformes herunder også, *hvorledes tilbudsgiver vil tage afsæt i eksisterende koncepter og materialer. *Herunder også bud på hvilke typer af konkrete værktøjer der vil være behov for i det uddybende materiale. Det er afgørende af der her er fokus på at materialet faktisk får virksomhederne til at udføre konkrete sikkerhedstiltag, se pkt. 1.4se pkt. 1.4
07	EK	Et oplæg til involvering af styregruppen og Erhvervsstyrelsen se pkt. 1.8.
08	MK	Beskrivelse af den endelige leverances format og struktur.
09	EK	Oplæg til hvordan sikkerhedstjekket når helt ud til virksomhederne, herunder også hvilke aktører, der inddrages og hvordan.se pkt. 1.4.
10	EK	Det skal dokumenteres, at den til opgaven prioriterede bemanding, har den nødvendige viden om og erfaring informationssikkerhed og med at kommunikere til målgruppen.