**Input voor het FOD Economie RRF SME Cyber Security project – Luik projectoproepen**

**HRZKMO/okt2021**

**VOORSTELLEN PROJECTEN**

|  |
| --- |
| **Projectvoorstel 1 – Sectorale trajecten** |
| **Korte omschrijving**  Door in het kader van sectororganisaties een werking op te zetten rond cyberveiligheid kunnen sectorgebonden aandachtspunten in kaart worden gebracht en, gebruik makend van het bestaande instrumentarium, via gerichte acties binnen de sector aangepakt worden. |
| **Omschrijving**   * Een beroepsorganisatie of een cluster van beroepsorganisaties binnen eenzelfde sector kunnen in een sectorale werkgroep cyberveiligheid onder begeleiding van een externe cyber security consultant werken rond het verbeteren van de cyberveiligheid van de kmo’s in de eigen sector. * Ook andere actoren van de productie- of dienstverleningsketen kunnen daar bij betrokken worden. * De aanpak van de cyberveiligheid kan ook plaatsvinden in het kader van de werking rond digitalisering binnen de sector * Op basis van enkele sectorale projecten kan er dan vervolgens ook een standaardtraject uitgewerkt worden dat als leidraad kan dienen voor andere sectoren. * Er kan gestart worden met het opstellen van een sectorale risk assessment. Op basis daarvan kunnen dan geïdentificeerde pijnpunten aangepakt worden. Daarvoor dient in de eerste plaats het bestaande instrumentarium gebruikt te worden. Daarnaast kunnen er specifieke webinars, trainings digitale informatiepagina’s en communicatie initiatieven opgesteld worden. * Een lopend project van The Hague Security Delta voor de greenhouse sector in Nederland kan hier als best practice dienen. * Sectorale pagina’s voorzien op de campagnesite |

|  |
| --- |
| **Projectvoorstel 2 – Quiz-platform** |
| **Korte omschrijving**  Gratis gebruik door kmo’s van platform waar zij bestaande quiz kunnen verspreiden onder hun personeel en de resultaten kunnen delen/opvolgen |
| **Omschrijving**   * De CSC heeft op het platform Kahoot een quiz over veilig thuiswerken gecreëerd: <https://www.cybersecuritycoalition.be/resource/interactive-cyber-security-elearning/> Bedrijven kunnen die quiz onder hun medewerkers verspreiden die het dan tegen elkaar kunnen opnemen. Dit platform heeft echter een aantal beperkingen. Momenteel bestaat er ook alleen nog maar een quiz over thuiswerken. * Er zou een beter geschikt platform gevonden of, indien dat haalbaar is, ontwikkeld moeten worden. * Er zouden twee extra quizzen moeten gemaakt worden over andere onderwerpen. * Het platform moet ook toelaten dat er nadien nog extra quizzen bij op geplaatst kunnen worden. |

|  |
| --- |
| **Projectvoorstel 3 – Awareness & training platform** |
| **Korte omschrijving**  Bestaand cyber security awareness & training platform gratis ter beschikking stellen van kmo’s. |
| **Omschrijving**   * Er bestaan goede platformen die door grote ondernemingen gebruikt worden voor de awareness & training van hun personeel. Deze platformen zijn ook voor kmo-ondernemers en hun personeel erg nuttig. * Het platform moet wel voldoende aangepast zijn aan hun werkcontext en gebruik maken van behavioural insights. |

|  |
| --- |
| **Projectvoorstel 4 – Phishing test platform** |
| **Korte omschrijving**  Bestaan phishing test platform gratis ter beschikking stellen van kmo’s.en content aanpassen aan hun werkcontext |
| **Omschrijving**   * Zoals grote bedrijven phishing tests organiseren onder hun personeel, kan dat ook nuttig zijn voor kmo’s * Hen gratis toegang geven tot bestaand platform met voldoende opvolgmogelijkheden * Hen daar voldoende aan hun werksituatie aangepaste phishing test mails bieden (per sector en taal) |

|  |
| --- |
| **Projectvoorstel 5 – Kmo’s op weg helpen naar cloudoplossingen** |
| **Korte omschrijving**  Kmo’s objectieve informatie geven over hoe de cloud voor hen een oplossing kan bieden |
| **Omschrijving**  Kmo’s zijn zich niet bewust van mogelijke voordelen op het vlak van cyberveiligheid van de cloud en hebben ook vragen inzake de cloud (wat is dat juist, soorten cloud, wel veilig, wat met GDPR?...). Daarom:   * opstellen objectieve informatie inzake voordelen en vraagstukken * dit verspreiden via animatiefilmpje, brochure, scan (vragenlijst met advies) |

|  |
| --- |
| **Projectvoorstel 6 – Automated scans** |
| **Korte omschrijving**  Kmo’s toegang geven tot tools die online hun pc, netwerk, website of webshop kunnen scannen op kwetsbaarheden en die op basis van de gevonden kwetsbaarheden acties voorstellen |
| **Omschrijving**   * Wat bestaat er momenteel reeds? * Zijn die tools niet te technisch voor kmo’s? Kunnen ze die zelf hanteren? * Kunnen deze ter beschikking worden gesteld van kmo’? * Informatie voor kmo’s hierover * Deze ter beschikking stellen |

|  |
| --- |
| **Projectvoorstel 7 – Gebruik technische bescherming door kmo’s bevorderen** |
| **Korte omschrijving**  Het gebruik van technische beschermende maatregelen door kmo’s bevorderen |
| **Omschrijving**   * Wat bestaat er momenteel reeds? * Zijn deze maatregelen niet te technisch voor kmo’s? Kunnen ze die zelf hanteren? * Kunnen deze ter beschikking worden gesteld van kmo’? * Informatie voor kmo’s hierover * Kan dat gebruik financieel ondersteund worden?   Het subsidiëren van dergelijke oplossingen moeten we wel kritisch bekijken aangezien we dat toch maar lichtjes zouden kunnen subsidiëren en we geen marketing acties voor private aanbieders willen organiseren. Waarschijnlijk is het beter om daar objectieve informatie over te ontwikkelen en te verspreiden of de subsidie te beperken tot specifieke groepen van kmo’s of te koppelen aan andere projecten zoals de werking binnen de sectororganisaties. |

|  |
| --- |
| **Projectvoorstel 8 – Incident response ondersteuning** |
| **Korte omschrijving**  KMO’s die het slachtoffer worden van een cyberincident informatie bieden over de stappen die zij moeten nemen door hen daarover duidelijke informatie ter beschikking te stellen en daarvoor een support desk op te richten. |
| **Omschrijving**  Kmo’s die het slachtoffer worden van een cyber incident (zoals bijvoorbeeld ransomware) weten vaak niet hoe ze deze situatie moeten aanpakken. De bestaande incident management guide is voor hen te complex en andere informatie die men online vindt is dan weer vaak te summier. Er is dus nood aan duidelijke informatie op maat van de kmo. Elke kmo en elk incident is bovendien ook verschillend. Naast algemene online informatie, is er dus ook nood aan individuele ondersteuning . Daarom zou er ook een gratis support desk voor kmo’s moeten komen die de kmo’s eerste lijn advies kan bieden over wat ze best doen in het geval van een incident.  Dus:   * Online informatie opstellen en aanbieden * Support desk |

|  |
| --- |
| **Projectvoorstel 9 – Cyberveiligheid integreren in het bestaande opleidingsaanbod voor kmo’s en hun personeel** |
| **Korte omschrijving**  Cyberveiligheid integreren in het bestaande opleidingsaanbod voor kmo’s en personeel, enerzijds door cyberveiligheid aan bod te laten komen binnen bestaande opleidingen over digitale toepassingen en anderzijds door afzonderlijke opleidingen over cyberveilige digitalisering binnen dat opleidingsaanbod aan te bieden. |
| **Omschrijving**  Cyberveiligheid moet meer deel uit maken van het bestaande opleidingsaanbod voor kmo’s en hun personeel in het kader van bijvoorbeeld de verplichte permanente vorming in bepaalde beroepen (bijvoorbeeld de boekhouders), de sectorale opleidingsfondsen, …   * Cyberveiligheid moet dan in de eerste plaats geïntegreerd worden in andere opleidingen, bijvoorbeeld inzake digitale toepassingen. Als je momenteel bijvoorbeeld in de bouwsector een opleiding volgt over het gebruik van een graafmachine dan gaat die opleiding ook over het veilig gebruik van die machine. Indien je een opleiding zou volgen over het gebruik van bepaalde bouwsoftware, dan zou het cyberveilig gebruik van die software ook aan bod moeten komen. * Daarnaast kunnen in sommige sectoren binnen het bestaande opleidingsaanbod ook afzonderlijke opleidingen over cyberveiligheid nuttig zijn maar die zouden dan ook ruimer en positiever kunnen omschreven en ingevuld worden en eerder kunnen gaan over bijvoorbeeld efficiënt en veilig digitaal werken.   Wat concreet doen?   * Screening om te kijken in welke mate cyberveiligheid momenteel reeds aan bod komt binnen het opleidingsaanbod voor kmo’s en hun personeel * Identificatie opportuniteiten / mogelijke acties om cyberveiligheid meer te integreren in dat bestaande opleidingsaanbod * Acties nemen om die integratie te realiseren (sensibiliseren, inhoudelijk ondersteunen, …) |

|  |
| --- |
| **Projectvoorstel 10 – Informatiesessies per sector** |
| **Korte omschrijving**  Het organiseren van een laagdrempelige informatiesessie over digitalisering en cyberveiligheid per sector. |
| **Omschrijving**  In bepaalde sectoren is er eenvoudigweg nood aan een eenvoudige en laagdrempelige informatiesessie over cyberveiligheid waarbij rekening gehouden wordt met de eigenheid van het beroep of de sector. Bovendien wordt dat best als deel van of samen met het onderwerp digitalisering behandeld. Het organiseren van dergelijke sessie is niet altijd eenvoudig voor de beroepsorganisaties van die sectoren (inhoud bepalen, sprekers vinden, praktisch, …). Vanuit dit project zouden ze daarbij kunnen ondersteund worden. |