



Marktconsultatie Cyber-Awareness programma

DCTerra

DATUM:	11-3-2024
VERSIE:	2.1
OPDRACHTGEVER:	HAN NUMAN
OPDRACHTNEMER(s):	ANNEMIEK ANNEN, PATRICK LUBBERS

INHOUD

Versiebeheer	3
Inleiding	4
Aanleiding	5
Huidige stand van zaken	5
Doel.....	6
Randvoorwaarden en beperkingen	7
Risico's	7
Relaties met andere projecten en kaders.....	8
Besluiten, middelen in tijd en geld	8
Planning Marktconsultatie	9

<i>Versie</i>	<i>Datum</i>	<i>Naam</i>	<i>Wijzigingen</i>
0.1	5-2-2024	Patrick Lubbers	1 ^e Opzet.
0.2	13-2-2024	Patrick Lubbers	1 ^e Concept ter beoordeling door Annemiek.
1.0	1-3-2024	Patrick Lubbers	1 ^e Definitieve versie ter aanbod aan Inkoop
2.0	6-3-2024	Han Prinsen	1 ^e Reactie Inkoop
2.1	08-03-2024	Annemiek Annen	Feedback afdeling Inkoop verwerkt

INLEIDING

DCTerra is een onderwijsorganisatie die is ontstaan uit de fusie tussen ROC Drenthe College (DC) en AOC Terra. De fusie is momenteel in volle gang en daarom wordt deze marktconsultatie geschreven vanuit het perspectief van DCTerra.

Informatie en ICT-faciliteiten dienen tegenwoordig 24/7 en vanaf elke locatie (online) beschikbaar te zijn voor zowel medewerkers als studenten. DCTerra dient informatie, ICT-faciliteiten en de toegang hiertoe optimaal te beveiligen. Kwaadwillende proberen 24/7 toegang te verkrijgen tot de ICT-omgeving van DCTerra om deze vervolgens te gijzelen of misbruiken.

DCTerra realiseert zich dat hacking een enterprise business is geworden. Wereldwijd vinden er meer dan 4000 ransomware aanvallen per dag plaats. Gemiddeld is iedere 11 seconden een nieuwe organisatie slachtoffer van een ransomware aanval. De wereldwijde schade is van \$88 miljard in 2018 gestegen naar \$208 miljard in 2022. Sinds de hack van de Universiteit Maastricht in 2019 staat het onderwijs ook op de aanvalslijst van de hackers en zijn diverse onderwijsorganisaties, inclusief ROC's, slachtoffer geworden van grootschalige datalekken en ransomware aanvallen.

Mensen zijn de zwakste schakel binnen cybersecurity. Hierbij is het gedrag van mensen het grootste risico binnen meer dan 90% van de wereldwijde cyberincidenten ontstaat door phishing en op andere wijze gelekte credentials.

Security/Cyber-awareness is het bewust en veilig omgaan met informatie en technologie. Awareness zorgt ervoor dat iedereen op een verantwoorde en veilige manier met technologie, informatie en gegevens omgaat en cyberincidenten worden voorkomen. Dit gaat van het omgaan met mobiele apparaten, veilig werken, het omgaan met persoonsgegevens tot het herkennen van zaken als social engineering, phishing en andere vormen van fraude.

Onbewust is de mens geneigd op basis van goed vertrouwen te reageren en handelen. Cyber-awareness is iets wat niet van nature aanwezig is of middels een eenmalige training wordt gerealiseerd. Het moet continu worden getraind om er bewust van te blijven en juist te leren handelen.

DCTerra is voornemens om tot een compleet cyber-awareness programma te komen binnen DCTerra waarbij rekening wordt gehouden met de diverse doelgroepen en behoeften binnen de organisatie. Middels deze marktconsultatie vraagt DCTerra om informatie omtrent de mogelijkheden en oplossingen welke geboden worden vanuit de markt.

AANLEIDING

Informatiebeveiliging- en privacy (IBP) gaat in eerste instantie over gedrag, cultuur en bewustwording. Pas hierna zijn technische maatregelen, fysieke toegang en ICT-onderdeel van IBP. Wanneer met deze informatie en ICT niet zorgvuldig wordt omgegaan kan dit leiden tot aantasting van de integriteit, vertrouwelijkheid en betrouwbaarheid van informatie en daarmee de continuïteit van het onderwijs.

Zowel vanuit wet- en regelgeving als vanuit eigen verantwoordelijkheid zoekt DCTerra een partner waarmee zij gezamenlijk met diens technologieën/portfolio een passend cyber-awareness programma gaat realiseren.

Sinds maart 2020 zijn de drie noordelijke ROC's (DC, Noorderpoort en Alfa College) een strategische samenwerking aangegaan als *DNA*. Hierbij is de ambitie gesteld om deze samenwerking steeds verder te laten groeien en te versterken. Om deze reden wordt in deze marktconsultatie rekening gehouden met verdere samenwerking met de DNA-partners.

HUIDIGE STAND VAN ZAKEN

Binnen DC en Terra zijn diverse initiatieven gestart m.b.t. het verhogen van de cyber-awareness. Deze initiatieven worden voornamelijk op ad-hoc niveau georganiseerd en worden niet structureel herhaald.

DC heeft in juni 2023 een awareness-meting laten uitvoeren in het kader van het programma 'Cyberveiligheid' van MBO Digitaal. De meting is uitgevoerd door BDO en opgedeeld in drie onderdelen, namelijk: motivatie, gelegenheid en bekwaamheid. Het gemiddelde eindcijfer van deze meting is 6.2 op basis van 86 respondenten. Echter stelt MBO Digitaal dat met een 7 gemiddeld een organisatie voldoende motivatie, bekwaamheid en gelegenheid heeft om privacy bewust en informatieveilig te werken.

De uitkomsten van de meting zijn als volgt samengevat:

- **Motivatie (6.3):**
93% van de respondenten geeft aan privacy en security belangrijk te vinden. Personeel besteedt hier aandacht aan, met voornaamste reden dat zij zich zouden schamen wanneer door hen een incident of datalek ontstaat. Daarnaast vindt men het belangrijk om DC digitaal weerbaar te maken.
- **Bekwaamheid (5.4):**
Dit onderdeel bestaat uit acht toetsvragen. Op drie van de acht toetsvragen wordt merendeels fout geantwoord. De volgende thema's komen naar voren als aandachtsgebieden: wachtwoordsterkte, social media risico's en datalekmeldingen.
- **Gelegenheid (7):**
66% van de respondenten vindt dat DC goed faciliteert om privacy-bewust en informatieveilig te werken. Een minderheid van de respondenten vindt dat leidinggevend het goede voorbeeld geven.

AOC Terra heeft geen nulmeting laten uitvoeren zoals DC.

DOEL

Het uiteindelijke doel van deze uitvraag betreft het realiseren van een meerjarig awareness plan voor de gehele organisatie van DCTerra, in voorbereiding op harmonisatie en aansluiting met DNA. Binnen dit awareness plan dient rekening te worden gehouden met de behoeften van de verschillende doelgroepen binnen de organisatie.

Dit project kent als resultaatgebieden:

- Inbedding en het meetbaar maken van informatiebeveiligingsbewustzijn binnen alle lagen van de organisatie met als deelgebieden:
 - Verhoging (cyber)awareness bij medewerkers en studenten.
 - Verhoging kennis van AVG bij medewerkers en studenten.

Voldoen aan vereisten, om op de relevante statements van het in “Relaties met andere projecten en kaders” beschreven in het NBA- en privacy-toetsingskader op het ambitieniveau, of hoger te scoren.

- Voldoen aan wet- en regelgeving rondom cyber- awareness.

Middels een professioneel awareness programma realiseert DCTerra integrale bewustwording rondom cybersecurity. Hierdoor worden hacks, misbruik en datalekken voorkomen of wordt schade tot een minimum beperkt. Het project en awareness programma richt zich op:

- De verschillende doelgroepen en hun behoeften, zoals:
 - MBO Studenten
 - VO Leerlingen
 - Medewerkers
 - Onderwijzend personeel
 - Ondersteunend & Beheers Personeel
 - Bestuur/management
 - Staff
 - HR
 - Financiën
 - ICT
 - Onderwijs Ondersteunend
- Realisatie van een meerjarenplanning met PDCA-cyclus om tot continue verbetering te komen.
- Medewerkers en studenten zijn geïnformeerd over de stand van zaken rondom awareness en eisen hierom binnen DCTerra.
- Medewerkers en studenten zijn beter weerbaar tegen misbruik door cybercriminelen, zowel in werk als privé situatie.

Het gewenste awareness programma houdt rekening met de verschillende doelgroepen binnen een organisatie of bedrijf en de context waarin deze functioneert. Zoals reeds beschreven kent DCTerra verschillende doelgroepen met verschillende behoeften. Het plan is erop gericht deze doelgroepen op een gepaste manier te scholen waardoor de adaptie naar verwachting groter zal zijn dan bij een algemene aanpak. Door het toepassen van periodieke herhaling zal het awareness niveau van de verschillende doelgroepen groeien.

Toepassing van een cyclische aanpak middels de PDCA-cyclus zal de organisatie in staat stellen om middels een cyclus van continue verbetering tot een steeds beter awareness programma te komen. Ook zal de aansluiting met de verschillende doelgroepen binnen de organisatie verbeteren door de continue evaluatie en aanpassing, wat wederom tot betere adaptie en awareness zal leiden. DCTerra wenst om tijdens de awareness training een

positieve benadering te hanteren, waarbij de focus ligt op succesverhalen en het toepassen van good-practices in plaats van een meer straffende aanpak.

Phishing campagnes en eventuele andere awareness-testen zijn onderdeel van dit programma, tezamen met meetbaarheid van de resultaten van het programma.

Implementatie wordt gefaseerd uitgevoerd per doelgroep. Op deze manier wordt de implementatie gefaseerd en beheersbaar uitgevoerd en kan tijdig worden bijgestuurd.

Tijdens de uitvoer van het voorgestelde project wordt meegenomen:

- De status van de awareness programma's bij de DNA-partners, de beschikbare materialen en mogelijke aansluiting hierop.
- De voorkeur van DCTerra t.o.v. het zelf realiseren awareness programma en/of content. Hierbij in acht te nemen dat DCTerra op ICT-gebied een strategie "buy before make" hanteert.
 - Voorwaarden en vereisten welke van toepassing zijn op beide scenario's.

RANDVOORWAARDEN EN BEPERKINGEN

Randvoorwaarden en beperkingen welke DCTerra erkent voor de awareness-campagne:

- **Commitment bestuur**
De werkwijze van het projectteam moet gedragen worden in de organisatie. Daarnaast moet het uitvoeringsplan waarmee het bewustzijn verhoogd wordt ook gedragen in de organisatie.
- **Geen vrijblijvendheid**
Deelname aan de awareness-campagne kent geen vrijblijvendheid om het effect, namelijk verhoogde bewustzijn, in noodzaak voor de organisatie af te dwingen.
- **Evaluaties**
Jaarlijks vinden evaluaties plaats om de effectiviteit van de campagne te toetsen en zo nodig aanpassingen door te voeren. Hiermee wordt herhaling geborgd.
- **Duidelijke planning**
Het projectteam levert een duidelijke planning op met start- en eindpunt, mijlpalen en andere belangrijke data.
- **Budget**
Indien de kosten inzichtelijk zijn, dient de organisatie voldoende tijd en middelen te reserveren om tot uitvoer van het awareness programma te komen.

RISICO'S

- **Budget/middelen**
Voor IBP en awareness is geen begroting vastgesteld. Hoewel er momenteel een awareness programma loopt, zijn de financiële middelen hiermee niet gegarandeerd. Voor het nieuwe programma dienen de juiste (financiële) middelen te worden vrijgemaakt. Om deze reden is het belangrijk middels dit marktonderzoek de te verwachten kosten in kaart te brengen.
- **Aanbestedingsplicht**
Afhankelijk van de kosten voor het awareness-programma, bestaat de mogelijkheid dat vanwege de omvang van de kosten een aanbesteding moet worden uitgevoerd. Een Tender vraagt zowel van de betrokken projectdeelnemers als de afdeling Inkoop extra inzet. Ook zal realisatie van het awareness-programma een langere doorlooptijd kennen.

RELATIES MET ANDERE PROJECTEN EN KADERS

De awareness-campagne heeft een directe relatie met andere projecten en toetsingskaders.

- **Fusie DCTerra**

Als antwoord op de krimp en de opgaven in de regio zijn AOC Terra en DC gefuseerd. Uit de voorafgaande Fusie-effect Rapportage is gebleken dat de instellingen een goede match zijn. Door samen uitdagingen op te pakken in plaats van te concurreren wordt een gezamenlijke strategische agenda opgezet met als doel de continuïteit van de gehele keten te waarborgen. In aanloop naar de instellingsfusie moeten veel beleidsstukken geharmoniseerd worden. Dit biedt mogelijkheden om het NBA-toetsingskader en het Privacy-toetsingskader te verwerken in de werkzaamheden.

De volgende toetsingskaders kennen een relatie tot de fusie en de awareness-campagne:

- **NBA-toetsingskader**

Veiligheidsbewustzijn is een onderdeel van het domein 'Personeelsbeheer' van het NBA-Toetsingskader. Dit kader wordt in het mbo-landschap sinds 2021 gebruikt om IBP in te richten. Daarnaast stelt het domein Bestuur dat awareness een onderdeel moet zijn van het IBP-beleid van een organisatie. In aanloop naar- en tijdens de fusie kunnen de statements van het kader herzien- en waar nodig aangevuld worden.

- **Privacy-toetsingskader:**

Het privacy-toetsingskader is nauw verbonden met het NBA-toetsingskader. Zo gaat statement OI.04 over bewustwording van privacy in de organisatie. In aanloop naar- en tijdens de fusie kunnen de statements van het kader herzien- en waar nodig aangevuld worden.

NBA-TOETSINGSKADER	PRIVACY-TOETSINGSKADER
GO.02 Beleid	BL.01 Privacy beleid
HR.02 Certificering, training en scholing	OI.01 (g) Aanwijzing en positie FG
HR.06 Veiligheidsbewustzijn	OI.02 (c) Privacy-organisatie
	OI.04 (a, b, c) Bewustwording

Tabel 1: Statements NBA en Privacy

BESLUITEN, MIDDELEN IN TIJD EN GELD

Aansluitend op het “make or buy” besluit waarbij de afdeling ICT & IM als regio voerende partner van de rest van de organisatie wordt ingezet en deze inzet op standaardisatie en het afnemen van diensten, stellen de opdrachtnemers voor om te onderzoeken hoe de markt de organisatie kan bedienen bij het realiseren van een awareness programma welke aansluit bij de behoefte zoals deze gesteld is.

Tijdens het onderzoek zal in kaart worden gebracht wat de behoefte van de organisatie is en hoe de markt kan aansluiten bij deze behoefte.

Nadat de behoefte in kaart is gebracht zullen de financiële consequenties worden geïnventariseerd. Hierbij wordt een onderscheid gemaakt in:

- Eenmalige kosten.
- Terugkerende kosten.

Vanuit de marktconsultatie wordt het volgende besluit genomen:

- Een “Go” of “No-Go” op uitvoering van het beschreven project ter realisatie van een integraal awareness-programma, waarbij de financiële en niet-financiële consequenties duidelijk zijn.

VRAAG AAN DE MARKT (BUSINESS CASE)

Vanuit bovengeschetste geschetste situatie wordt gevraagd informatie te geven over de volgende vraag:

Op welke wijze kan uw organisatie DCTerra helpen met het verhogen van de cyber-awareness binnen de verschillende doelgroepen om de gewenste resultaten te bereiken?

Geef hierbij aan:

- Het verwachte tijdpad
- De voorgestelde aanpak
- De gespecificeerde kostenindicatie

PLANNING MARKTCONSULTATIE

ACTIVITEIT	DATUM
Publicatie marktverkenning via TenderNed	11 maart 2024
Deadline tot het stellen van vragen over de inhoud marktconsultatie	3 april 2024
Beantwoording DCTEerra op gestelde vragen over inhoud marktconsultatie	5 april 2024
Indienen antwoord op 'Vraag aan de markt' business case	19 april 2024
Sluitingsdatum beoordeling business case	26 april 2024
Publicatie verslag marktverkenning incl. besluit al dan niet aan te besteden	17 mei 2024