HEIDAG
CIO-RAAD VWS

START

MENU

! *Navigeer door op één van de onderdelen uit het menu te klikken of klik op start. Vanuit een hoofdstuk keer je terug naar het menu door op de menu knop bovenaan te klikken.*

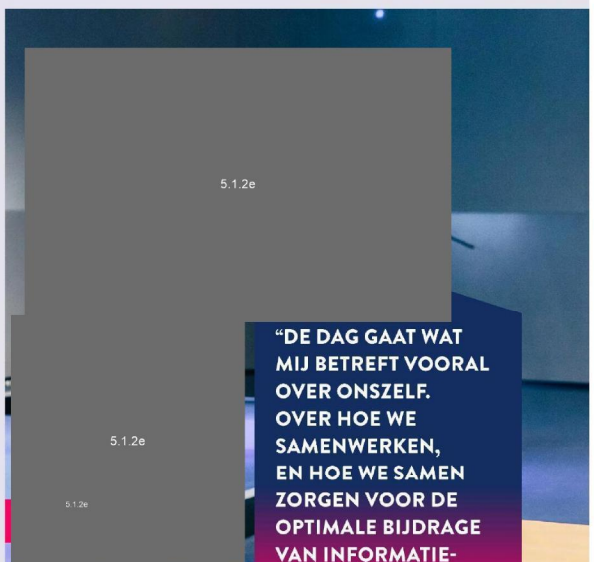
1

WELKOMSTWOORD

Een dag organiseren waar Chief Information Officers en liaisons van het ministerie van Volksgezondheid, Welzijn en Sport en de concernonderdelen bij elkaar komen. Dat gebeurde tijdens de heidag op 15 september 2020. Een informatieve en productieve middag creëren door kennis op te halen en te delen, vanuit ieders eigen functie. 5.1.2e, directeur informatiebeleid en CIO van het ministerie van VWS trapt de dag af en brengt alle presentaties gedurende de dag samen.

De onderwerpen die deze middag aan bod komen zijn actueler dan ooit: cyber security, informatieveiligheid en CoronaMelder. Door de razendsnelle ontwikkelingen van technologie en de complexiteit van de markt moet er continu scherp gekeken worden naar systeem-beveiliging. Is er een fout of een lek? Dan heb je een probleem, want binnen no time ligt er een DDoS-aanval op de loer. Hoe goed kunnen organisaties dan beveiligd worden, welke mogelijkheden zijn er binnen de wet- en regelgeving in Nederland, hoe wordt een waterdicht systeem gerealiseerd en op welke risico's moet er dan worden ingespeeld?

5.1.2e houdt de opening van deze heidag kort maar krachtig: "De dag gaat wat mij betreft vooral over onszelf. Over hoe we samenwerken, en hoe we samen zorgen voor de optimale bijdrage van informatievoorziening aan onze opgaven. Wat leren we van elkaar en hoe integreren we deze leerpunten in ons eigen werk? Lukt het ons om ervoor te zorgen dat we ons werk nog beter uitvoeren en elkaar helpen waar mogelijk. Binnen VWS, maar ook hemelsbreed."



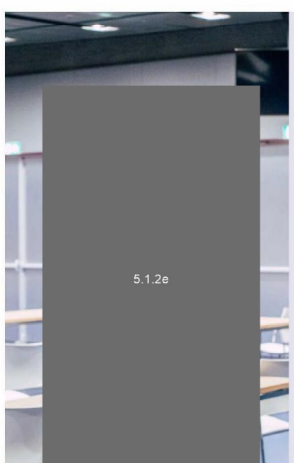
MENU

BEZOEKERS AAN HET WOORD

5.1.2e

5.1.2e

"Als we met z'n allen op dezelfde manier kunnen acteren, bouwen en daarin dezelfde taal spreken, zorg je voor afstemming en kost het vertalen naar wat je doet minder tijd. Ik denk dat het goed is om informatie te delen, maar dat het ook krachtig kan zijn wanneer een ander VWS-onderdeel jouw werk bekijkt. Zo kun je zien of hetgeen wat jij hebt gemaakt haalbaar is en of het dezelfde uitkomst geeft. Als je dan een soortgelijke bevinding hebt, kun je elkaar vervolgens gaan helpen."



5.1.2e

CISO BIJ ZORGINSTITUUT NEDERLAND

"Deze heidag zie ik als onderdeel van een goede informatievoorziening en daar staan wij voor. De onderwerpen die vandaag langskomen, zijn namelijk vraagstukken waar we allemaal tegenaan lopen. Daarnaast is het doel, binnen het CIO-verband, meer interdisciplinair samen te werken. Elkaar beter te leren kennen en kennis en kunde met elkaar te delen, lijkt mij een goed idee."

2

DE **CYBER RISICO'S** IN BEELD

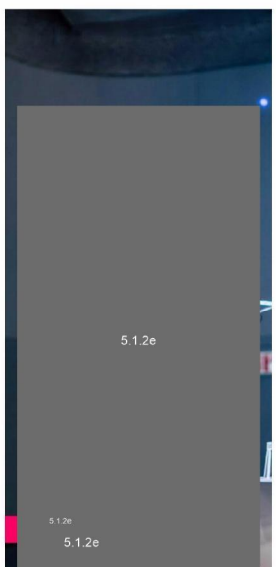
5.1.2e **heeft ruim twintig jaar ervaring op het gebied van informatie-beveiliging, IT en cybersecurity (en karate als hobby). Met deze hoeveelheid aan ervaring weet hij precies hoe risico's te analyseren en hierop in te spelen. Als Chief Information Security Officer bij het Rijksinstituut voor Volksgezondheid en Milieu is het nu extra belangrijk om scherp te zijn op de bijbehorende privacy- en veiligheidsrisico's rondom het coronavirus.**

PAK DE KWETSBAARHEDEN AAN

Om risico's in kaart te brengen zijn er meerdere dingen nodig, onder andere het analyseren van de dreigingsbeelden. Deze dreigingen zijn vaak te vinden in de kleine kwetsbaarheden, denk aan een ontevreden medewerker of een georganiseerde aanval van binnenuit. 5.1.2e "Het is belangrijk om dit dreigingsbeeld te delen met elkaar. Deze analyse heeft een wollig karakter, maar we zijn ermee bezig om dit concreet en tastbaar te maken."

Vergeet niet de meest recente kwetsbaarheden en cyberrisico's. Door corona werkt bijna iedereen thuis op een laptop. Wat doet het thuiswerken met de veiligheid? En hoe zit dit in de zorgsector? Welke tools zijn wel of niet betrouwbaar?

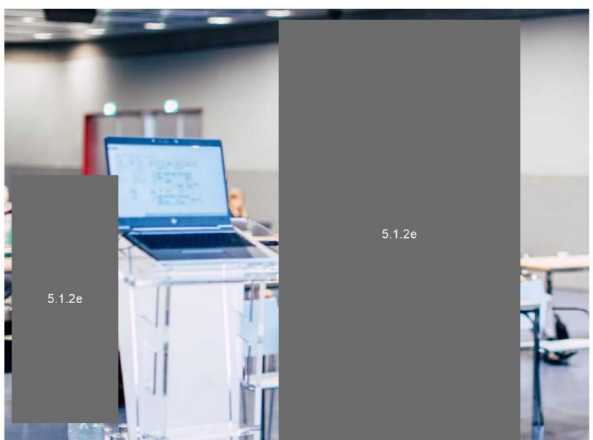
"Het gaat ook om de betrouwbaarheid van je data", volgt er uit de groep. Er is duidelijk behoefte naar het vinden van balans in risicobeperking. Zo kijkt het RIVM steeds naar manieren om risicomanagement in te zetten, gaat Bart verder. Neem



bijvoorbeeld de QuickScan: "Deze voeren we periodiek en bij grote wijzigingen uit op alle processen. Wat hieruit komt, bepaalt ook gelijk of we de risicoanalyse moeten inzetten."

RISICOANALYSE ANNO 2020

Deze risicoanalyse-methodieken zijn nodig, om de steeds nieuwere technologie bij te houden. Een cybercrime-methodiek, zoals we nu gebruiken, bestond voor 2017 nog niet. Er wordt dan ook verwacht dat deze methodiek aansluit op het huidige dreigingsbeeld en goed functioneert binnen het informatierisicomanagement. Om snel in te haken op veranderingen, is het belangrijk te werken in meerdere fases. 5.1.2e "Je ziet in organisaties dat er veel kennis zit in de hoofden van mensen. Documentatie ontbreekt daardoor vaak. Het is belangrijk dat je samen onder andere een systeemdecompositie maakt. Zo houd je elkaar scherp en zorgt het voor een verdiepingsslag."



“DE RISICOANALYSE EN DE QUICKSCAN ZIJN HANDIGE MIDDELEN, DIE VOOR ONS GOED WERKEN. ZO KAN DIT MISSCHIEN OOK VOOR EEN ANDERE ORGANISATIE WERKEN.”

MENU

“En hoe doe je dat dan met applicaties die je standaard koopt van de leverancier?”, vraagt iemand uit de groep. 5.1.2e haalt Microsoft Teams aan en vertelt waar het toolgebruik als basis in de risicoanalyse staat. “Zodra er dan nieuwe iteraties komen op deze tool, geef je alleen weer wat er nieuw is en doe je daar je assessment op.” Na de implementatie wordt dan gelijk getest of de maatregelen ook daadwerkelijk werken. Dit testen moet met meerdere mensen tegelijk, om vervolgens een dialoog aan te gaan en te kijken hoe zwaar elk onderdeel gewogen moet worden.

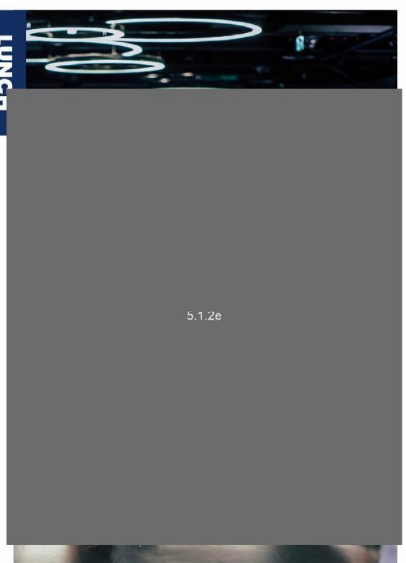
Maar hoe zorg je ervoor dat dit soort risico’s tijdig worden geanalyseerd? Wat is het juiste moment en hoe bepaal je dat moment? “Je moet zorgen dat je binnen alle lagen van de organisatie goed communiceert met elkaar”, gaat 5.1.2e verder. Dit is een manier van werken die voor elke situatie weer een andere aanpak vereist. “Het op tijd aanhaken blijft een ‘gevecht’, omdat er soms andere belangen zijn”, volgt uit de groep. Iemand anders vult aan: “De kunst is om op tijd aan te haken in een project, anders blijft het een soort eindexamen waar je altijd weerstand tegen hebt.”

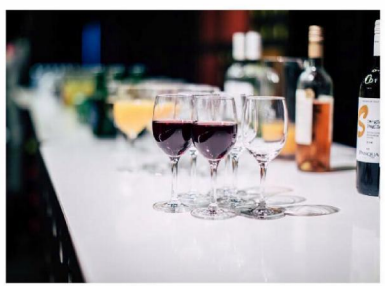
“OM TIJDIG RISICO’S TE KUNNEN SIGNALEREN MOET ER TRANSPARANTIE ZIJN. DAT VRAAGT TIJD, INZICHT EN NOODZAAK”

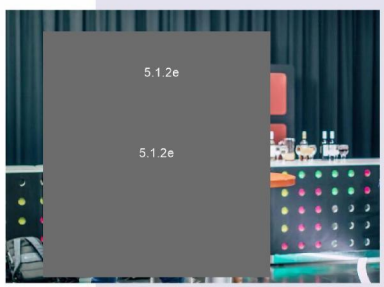
5.1.2e sluit het onderdeel af met stof tot nadenken: “De uitdaging bij de overheid is dat we ons soms zodanig op processen focussen dat de uitvoering erg ingewikkeld wordt. Ik zou het mooi vinden als we een inhoudelijke lat leggen, waarbij we zelf blij worden van een systeem/proces en we binnen het concern VWS een paar mensen hebben die in staat zijn om te controleren of dit echt in de praktijk werkt. Dit moet er dan voor zorgen dat niet alleen processen worden nageleefd, maar dat er ook gekeken wordt naar een goed uitvoerbare implementatie.”

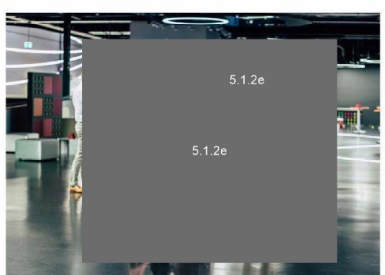
MENU

LUNCH









3

VAN CYBER RISICO TOT **VIRUSEPIDEMIE**

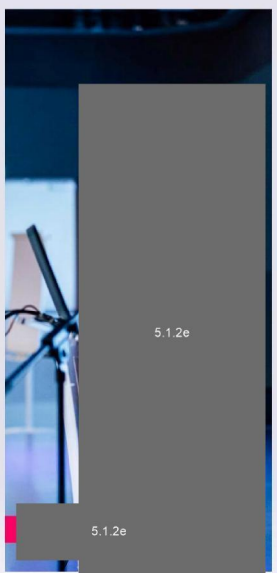
5.1.2e bij het ministerie van Volksgezondheid, Welzijn en Sport, hoopt de aanwezigen vandaag bewust te maken van het feit dat er veel organisaties zijn die cyberrisico's stapelen. Hij biedt de deelnemers van de heidag tijdens zijn sessie een aantal suggesties voor risicospreiding. Hoe gevoelig zijn systemen voor cyberaanvallen, welke cyberrisico's zijn er, waarom zijn ze besmettelijk en wat kun je hiertegen doen?

De knelpunten schetst 5.1.2e direct helder; IT-security is een moeilijk vakgebied. Binnen dit vakgebied neemt de rekenkracht toe, wordt de Gartner Hype Cycle korter en is er door schaalvergroting slecht zicht op misbruik en kwetsbaarheden. Met als gevolg het floreren en professionaliseren van cybercriminaliteit.

Hoe zijn we in staat de kwetsbaarheden goed te managen? En wat betekent dit voor de gekoppelde systemen waar we met z'n allen gebruik van maken? Henk-Jan legt uit: "We hebben een slecht beeld van hoe ICT meegaat met de snelheid van nieuwe apparaten. Oude apparatuur wordt op een gegeven moment niet meer geüpdatet, hoe veilig is het gebruik van deze apparatuur dan nog? Cybercriminelen hebben aan een lek voldoende, als organisatie moet je dus zorgen dat al deze gaten dicht zitten."

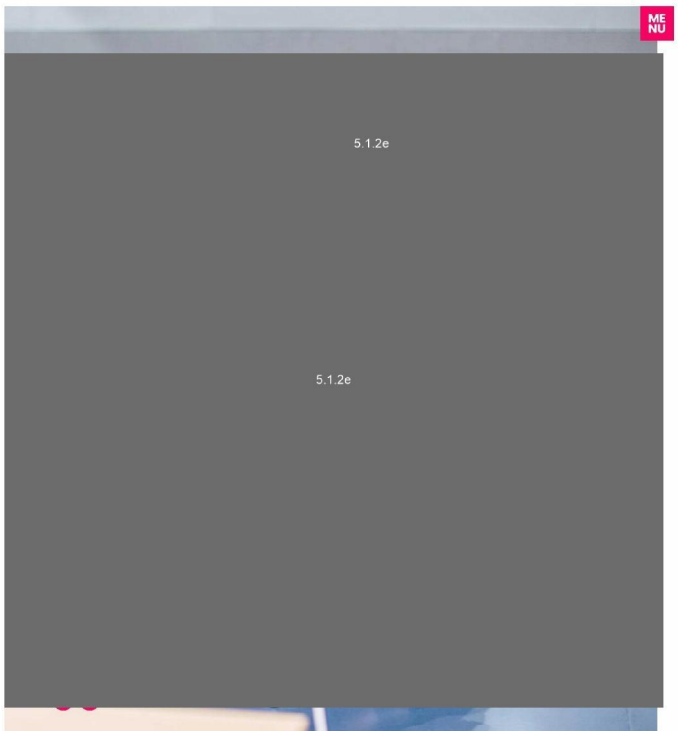
DRUK OP ANTIVIRUSSYSTEMEN

Computervirussen ontwikkelen zich snel, waardoor er ook een enorme druk komt op antivirussystemen. Cybercriminaliteit



wordt steeds meer een dagelijkse bezigheid, waardoor organisaties nu soms achter de feiten aanlopen. De meeste organisaties hebben 56 dagen nodig om virussen te ontdekken. Dit is al veel sneller dan voorheen, maar nog steeds niet snel genoeg om de gevolgen te beperken. Net als een cyberaanval die gemakkelijk kan plaatsvinden bij software die niet binnen 38 uur gepatcht is. "Patchen is iets wat snel moet plaatsvinden, om kwetsbaarheden te voorkomen. Hetzelfde geldt voor meer ICT-diversiteit, wat nodig is voor hogere software weerbaarheid", vertelt 5.1.2e

"ONDERTUSSEN BIEDT ANTIVIRUS OOK GEEN GARANTIE MEER, OMDAT ZE DE MEESTE NIEUWSTE VIRUSSEN NIET DETECTEREN."



DE SOFTWARE MONOCULTUUR

Organisaties maken steeds meer gebruik van dezelfde systemen. Dit biedt aan de ene kant voordelen, omdat er eenzelfde hoge kwaliteit is aan ICT-diensten of schaalvoordelen zijn bij de aanschaf van softwarelicenties. Aan de andere kant maakt het ook kwetsbaar, omdat er langzaam een software monocultuur wordt gecreëerd. En hoe besmettelijk moet een computervirus dan zijn om voor een ICT-virusepidemie te zorgen? De oplossing ligt volgens 5.1.2e in de benadering van een dergelijke epidemie: "Er zijn wel conventies bij normale plagen en epidemieën, maar waarom is er geen conventie bij ICT-epidemieën?"

Deze software monocultuur is iets wat heel Nederland aangaat. Belangrijker nog, hoe komt een land hier dan weer vanaf? 5.1.2e 5.1.2e eg uit: "Dat is kijken naar wat er per organisatie belangrijk is. Als er kritieke systemen in Nederland zijn, weten we dan hoe dat komt? En is hier een Single Point of Failure aan te wijzen?" De boodschap is helder, maar wie bepaalt nou welke risico's acceptabel zijn en welke niet? Is het acceptabel om bij een risico vijf dagen uit te vallen of moet er dan worden overgegaan op andere software? "Bepalen wat acceptabel is, kun je niet in je eentje doen. Dit moet je samen doen", vult 5.1.2e aan.

5.1.2e haakt aan waar 5.1.2e eindigt: "Ga met elkaar in gesprek, bevraag elkaar hierover tijdens de lunch. Denk bijvoorbeeld na over hoe we het nu organiseren en hoe jij dit zelf zou doen?"

MENU

BEZOEKERS AAN HET WOORD

5.1.2e
5.1.2e

“Mijn studieachtergrond is culturele antropologie. Ondanks dat mijn Rijkstraineeship niet volledig aansluit bij mijn achtergrond, vind ik het wel heel interessant. Je wordt namelijk overal mee naartoe genomen en bij betrokken. Door deze werkwijze word ik aangezet om creatief te zijn en denk ik na over hoe ik deze toch wel onbekende wereld kan laten aansluiten bij mijn eigen interesses en expertise. Zo kan ik vanuit mijn achtergrond een andere blik toevoegen. Bijvoorbeeld aan thema’s en discussies rondom privacy en cyber security.”

5.1.2e

“Ik heb vaak vakinhoudelijk contact met collega’s van informatiebeveiliging en wat minder met CIO’s, die op een andere manier met informatiebeveiliging en -beleid bezig zijn. Ik zie deze heidag daarom als een kans om van elkaars werelden te horen. In ons vak moet 100% beveiliging denk ik niet het doel zijn. Wel moeten er weloverwogen keuzes worden genomen om risico’s te beperken en de juiste mensen horen daarvan op de hoogte te zijn.”

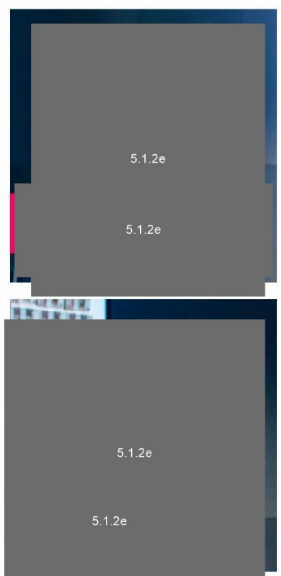
4

HET ONTSTAAN VAN **CORONAMELDER**

Dit jaar wordt de wereld getart door een infectieziekte en in Nederland ontstond de drive om dit zo snel mogelijk te bestrijden. Maar hoe doe je dat op een juiste manier? Cultuur, gedrag en kennis staan tegenover de harde cijfers van het aantal besmettingen. Er lijkt geen tijd te verliezen en dan wordt er gevraagd om een app te maken. 5.1.2e **, directeur informatiebeleid en CIO bij VWS, vertelt de aanwezigen hoe dit proces eruitzag en welke uitdagingen dit met zich mee bracht.** 5.1.2e **"Ik ben gevraagd om dit te gaan doen en ik zei; ik doe dit alleen als het mag met de allerbeste mensen. Dit mocht en ik ben de allerbeste gaan verzamelen." In het proces rondom de ontwikkeling van CoronaMelder haakte ook** 5.1.2e 5.1.2e 5.1.2e **aan.**

WERKEN MET DE ALLERBESTEN

Het ontwikkelen van CoronaMelder verliep niet geheel vlekkeloos. 5.1.2e drukt de groep dan ook op het hart om een hoger doel te hebben. "Als je niet kunt uitleggen wat het doet, dan krijg je mensen niet mee", vertelt 5.1.2e Dit viel onder andere op tijdens de Appathon. Dit leek heel effectief te zijn, maar dit was het uiteindelijk niet. Ron omschrijft het als een inschattingsfout: "Wij gingen ervan uit dat als je iets uitrolt binnen een land, zoals de Appathon, het wel gelijk zijn vruchten zal afwerpen." Het was namelijk niet de bedoeling om zo snel mogelijk een app te maken, maar om een héél goede app te ontwikkelen. En als er dan gewerkt wordt met de allerbeste mensen, komt die snelheid er vanzelf.



"WE WERKEN BIJ CORONAMELDER MET DE ALLERBESTE MENSEN EN IEDEREEN DIE MEE WILDE DOEN KON DAT DOEN. HONDERDEN DEVELOPERS EN DESIGNERS DEDEN DAT. DAT IS OPEN SOURCE TO THE MAX."

5.1.2e

MAAK HET PERSOONLIJK

Om er voor te zorgen dat CoronaMelder een goede app werd, werkten er alleen mensen aan die de inhoud ook voldoende snapten. Niet alleen de technische kant is namelijk belangrijk geweest in de totstandkoming van CoronaMelder, maar ook de psychologische kant. Vanaf het begin is de app heel persoonlijk ingestoken. Denk aan de opbouw van de app, welke is getest bij mensen met een visuele beperking of het design dat is voorgelegd via een poll op

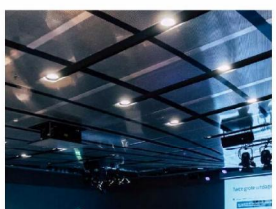
Twitter. Altijd stond de gebruiker centraal en werd deze bij het proces betrokken 5.1.2e legt uit: "Als de benadering persoonlijk is, gaan mensen het minder hebben over 'de overheid'. Het gesprek is daardoor beter te voeren, waardoor mensen de app mogelijk ook sneller gaan gebruiken."

GELEERDE LESSEN

De app CoronaMelder ligt onder een vergrootglas, waardoor het belangrijk is om de juiste keuzes te maken ten aanzien van het waarborgen van de privacy. Zo is de keuze gemaakt om gegevens niet te laten tracken. Sterker nog, CoronaMelder is de enige overheidsapp- of site waar geen tracking op staat. 5.1.2e ertelt over de weerstand die dit bracht vanuit de marketinghoek en hoe lastig het is om met alle goede bedoelingen een app voor heel Nederland te maken. "De mail over het verplicht downloaden van CoronaMelder had natuurlijk nooit gemogen. Ook al was het doel heel simpel; zou je eens willen kijken naar CoronaMelder?", legt 5.1.2e uit.

KRITISCH KIJKEN NAAR BEVEILIGING

De beveiliging van de app gebeurt op meerdere manieren. Dat is goed, maar hoe veilig zijn deze manieren? Het is wel een app die moet worden gebruikt door heel Nederland. Zo zijn er pentesten, maar geven deze ook garantie op volledige betrouwbaarheid, aangezien het een momentopname is? Om de app nog meer beveiligingskracht te geven, onderzoekt Secura de broncode van de app. Secura controleert de veiligheid van de app op mogelijke 'achterdeurtjes'. De beveiliging en privacy van CoronaMelder is nog niet volledig ingericht en daarom extra belangrijk om scherp te zijn op de kwetsbare plekken van deze app.5.1.2e concludeert: "Maar de kern van het proces zit goed. Alles is super transparant gemaakt en laat het echte verhaal zien." "Het verhaal is gewoon een kloppend verhaal", vult 5.1.2e aan.



5.1.2e

"EEN BELANGRIJKE KEUZE BIJ DE ONTWIKKELING VAN DE APP CORONAMELDER, WAS OM DE GEGEVENS NIET TE LATEN TRACKEN."

5.1.2e 5.1.2e 5.1.2e

5

IT TAKES THREE TO TANGO

Waar verschillende presentaties en onderwerpen passeerden, is het nu tijd om deze informatie om te zetten naar acties. Waar loopt iedereen tegenaan en is hier op de korte termijn een oplossing voor te vinden? Door middel van de thema's zoals Application Lifecycle Management, Portfoliomanagement en Data & Algoritmen, probeert 5.1.2e **van de directie Informatiebeleid/CIO van VWS, kaders mee te geven. Er worden vier groepjes gevormd, met elk een mooie mix van verschillende functies.**

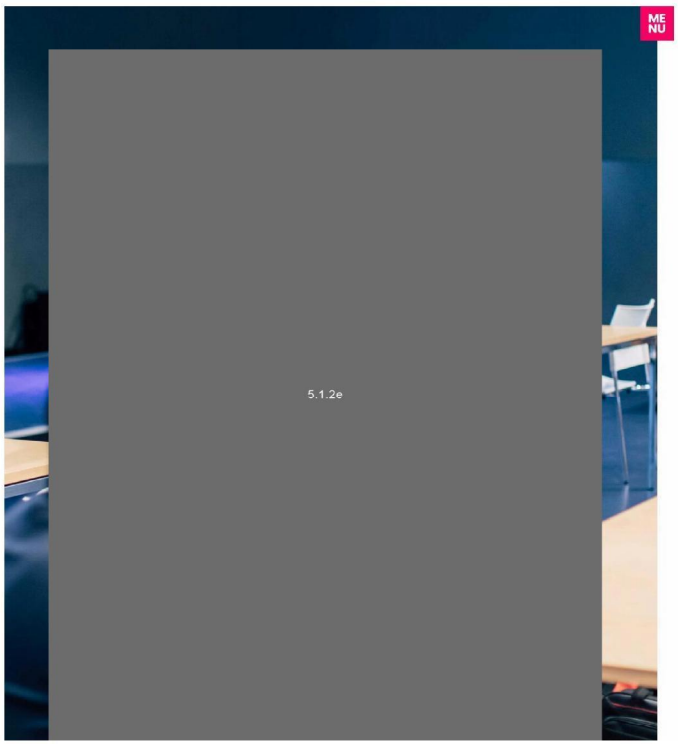
IN GESPREK MET DE LIAISONS, CIO-RAAD EN DE IBX

Er is behoefte aan dit moment, waar kennis en ervaring met elkaar gedeeld worden: "Ik mis een plek om online voorbeelden te delen". Doordat er veel thuis wordt gewerkt, is het niet altijd makkelijk te weten wat er speelt of waar mensen tegenaan lopen. Dat kost nu meer tijd en energie. Het zou helpen als de CIO's en de liaisons elkaar meer opzoeken. "Het begint met de vraag; weten we elkaar te vinden en blijven we elkaar vinden? Dat gebeurt nu nog te weinig."

GEMENE DELER

Alle groepjes formuleren unaniem hetzelfde doel: "Op de korte termijn zou een digitale samenwerkingsruimte via een platform enorm helpen." Via concrete vragen en portfoliomanagement komen tot een samenwerkingsomgeving, waarbij elkaars expertise effectief wordt gedeeld. "Zo'n soort platform komt alleen tot leven als je er wat komt halen en wat komt brengen", wordt beaamd. Een plek waar iedereen bij kan en die makkelijk te benaderen is, zodat mensen die elkaar nodig hebben elkaar makkelijk en snel kunnen vinden.

"JE KUNT JE NIET MET ALLES BEMOEIEN EN BIJ ALLES BETROKKEN WORDEN, MAAR ELKE FRISSE BLIK IS AL WINST."
GROEP 1



Een gevoel van bouwen aan een 'community' wordt genoemd: "Klein starten, daarna de rest laten aanhaken en uitbouwen."

KORTE TERMIJN

Om in actiepunten te denken, is het beginnen met een appgroep een goede eerste stap. Samenwerking heeft in deze tijd namelijk een zetje nodig. Net zoals het goed inrichten van wat er al is, zoals de TIPCO-tool. De groep vult aan: "En maak ruimte bij afdelingen binnen VWS om hier stappen in te zetten".

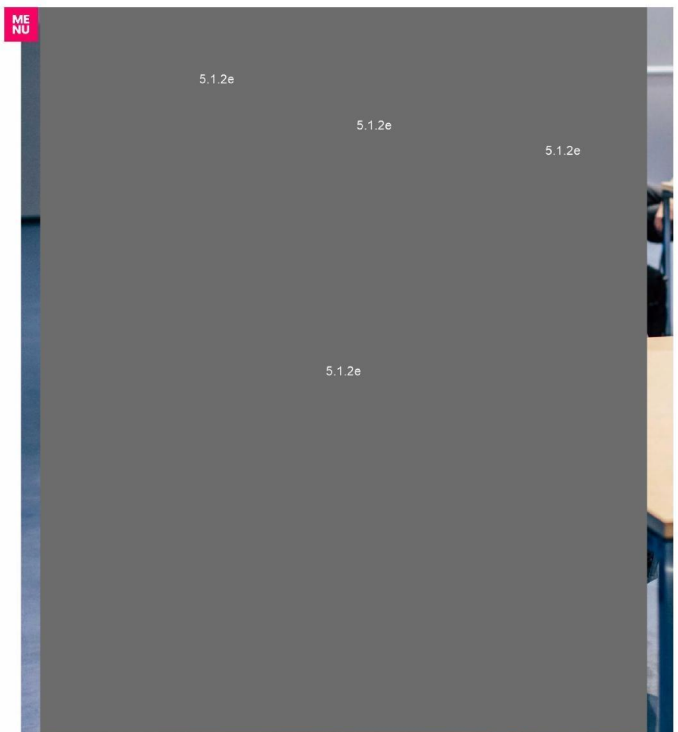
Iedereen is klaar om met enthousiasme te werken aan de communicatieverbetering binnen VWS-concern. Bereid om zich hiervoor in te zetten, zich kwetsbaar op te stellen en om de wil laten zien om een ander te helpen. De slotconclusie luidt: "We kunnen zelf het wiel opnieuw gaan uit vinden, maar het is veel beter om de bestaande kennis en kunde binnen VWS-concern nog beter met elkaar te delen."

"ALS JE MET EEN VRIJ GROTE GROEP BIJ ELKAAR ZIT, MOET ER VERTROUWEN ZIJN. OM PROBLEMEN EN DILEMMA'S BIJ ELKAAR NEER TE DURVEN LEGGEN EN OP TE LOSSEN."
GROEP 2

6

AFSLUITING

5.1.2e bij VWS) sluit het onderdeel en daarmee de heidag kort, krachtig en positief af: “We noemen deze samenwerkingstools al vaker, maken het steeds concreter en het zou geweldig zijn als we dit nu echt gaan realiseren met elkaar!” Een samenwerkingsplatform moet er komen. “Op een laagdrempelige manier, waar je snel in en uit kan”, vat 5.1.2e amen. Via portfoliomanagement moeten we elkaar inspireren om ons werk nog beter en eenvoudiger te doen. 5.1.2e sluit af: “En als het nodig is om hier een nieuwe bijeenkomst voor te organiseren, vraag het dan vooral aan me. Dan gaan we dat namelijk regelen!”



MENU

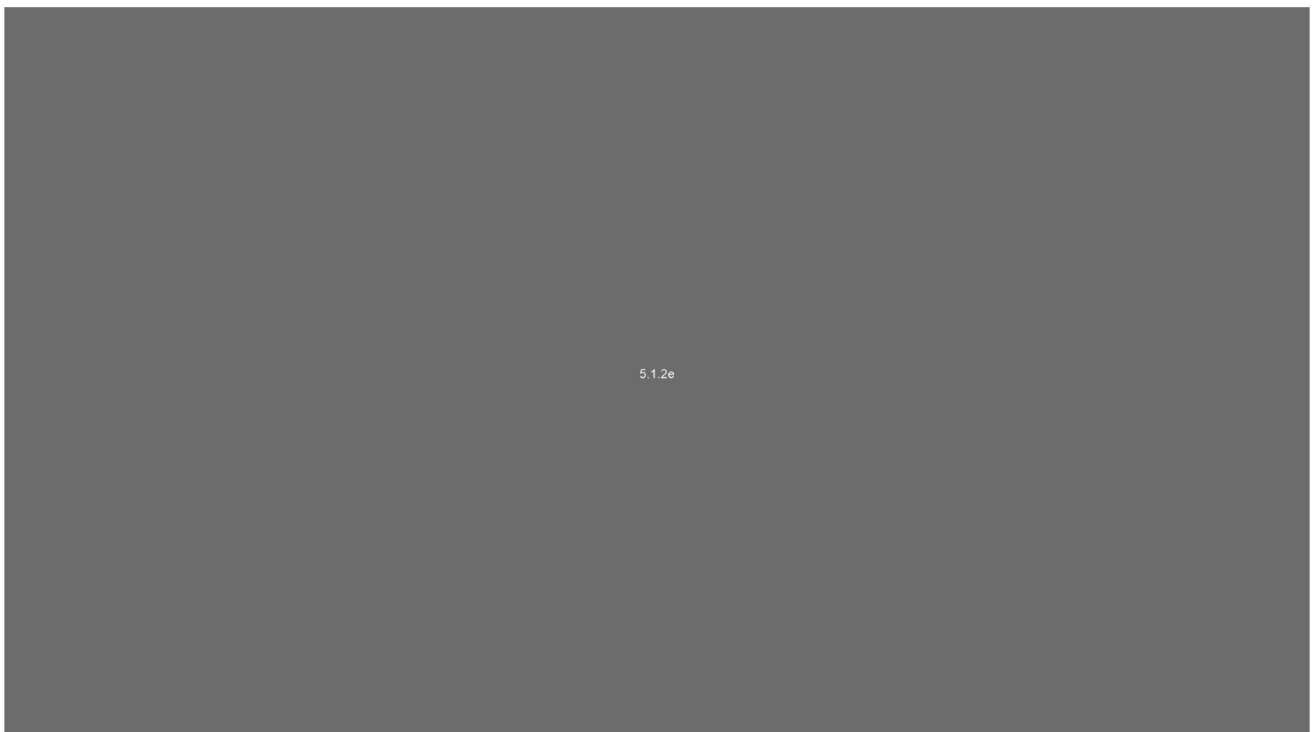
BEZOEKERS AAN HET WOORD

5.1.2e

“Sinds corona zijn er verschillende initiatieven gestart, de app CoronaMelder is er daar één van. Geweldig om te mogen zien hoe er in deze tijd wordt samengewerkt. Ook als CIBG hebben we daaraan mogen bijdragen. Zo hebben wij in drie en een halve week neergezet waar je normaal gesproken blij bent als het in drie maanden lukt. De urgentie was er natuurlijk voldoende, maar dan moet je het nog wel zo snel mogelijk tot een succes maken. Zo zie je dat je in een spanningsveld zoals deze, veel dingen snel en goed voor elkaar krijgt. Er is dan namelijk een heel andere samenwerkingsdynamiek. Voor nu is het belangrijkste dat de app helpt bij het bestrijden van de verspreiding van het coronavirus.”

5.1.2e

“We hebben elkaar vooral virtueel gezien de laatste tijd, in plaats van live. Dan gaat het vooral om het overleggen zelf, de stap naar buiten maken is er dan niet, terwijl ik denk dat het goed is dat we dit gezamenlijk verder brengen. Vanuit VWS komen er heel veel zaken op ons af en ik denk dat het daarom goed is dit gezamenlijk op te pakken. Het oppakken van nieuwe activiteiten geeft dan automatisch meer energie.”


5.1.2e