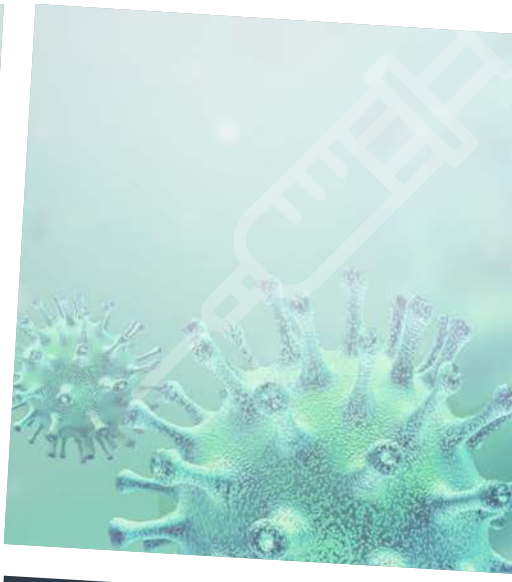
WAT IS DE INVLOED VAN EEN CYBERINCIDENT OP HET PATIËNTVERTROUWEN?

EEN FLITSONDERZOEK NAAR HET VERTROUWEN IN DE GGD CORONATESTSTRATEN EN BRON- EN CONTACTONDERZOEK NA EEN DATADIEFSTAL



Auteurs:

Jetze Dalmeijer

Jelle Groenendaal

Datum:

Juni 2021

let's change
YOU. US. THE WORLD.

DE HAAGSE HOGESCHOOL

Wat is de invloed van een cyberincident op het patiëntvertrouwen?

Een flitsonderzoek naar het vertrouwen in de GGD coronateststraten en bron- en contact-onderzoek na een datadiefstal

Dit flitsonderzoek is uitgevoerd door het Kenniscentrum Cybersecurity, Lectoraat Risk Management & Cybersecurity, Haagse Hogeschool, Den Haag in samenwerking met I&O Research, Amsterdam.

Auteurs:

Jetze Dalmeijer

Jelle Groenendaal

Datum: 1 juni 2021

INTRODUCTIE

Op 25 januari 2021 maakt RTL Nieuws[1] op basis van een uitgebreid onderzoek bekend dat er grootschalig gehandeld wordt in de miljoenen adresgegevens, telefoon- en burgerservice-nummers uit de coronasystemen van de GGD GHOR. Volgens RTL Nieuws werden de gegevens gestolen uit twee specifieke systemen: CoronaIT, waar de privégegevens van Nederlanders die een coronatest hebben gedaan in staan, en HPZone Lite, het systeem voor het bron- en contactonderzoek van de GGD GHOR.

Dezelfde dag maakt de GGD GHOR bekend[2] dat twee medewerkers van het landelijke coronatest afsprakennummer aangehouden zijn op verdenking van datadiefstal. Volgens de GGD GHOR zouden zij tegen betaling persoonsgegevens uit de GGD-systemen hebben aangeboden en daarmee uit zijn om persoonlijk gewin te halen uit de gegevens van mensen die zich hebben laten testen op het coronavirus. Later maakt de politie bekend dat er nog meer personen zijn aangehouden.[3]

> Uit het onderzoek van RTL Nieuws komt naar voren dat via chatdiensten als Telegram, Snapchat en Wickr enkele maanden privégegevens uit de GGD-systemen door tientallen accounts en in verschillende grote chatgroepen te koop worden aangeboden. Sommige accounts bieden volgens RTL Nieuws aan om de gegevens van een specifiek persoon op te zoeken. Dat kost tussen de 30 en 50 euro en dan ontvang je van iemand het woon- en mailadres en telefoon- en burgerservicenummer. Andere accounts bieden volgens RTL Nieuws grote datasets aan met daarin de privégegevens van duizenden Nederlanders. De criminelen vragen hier volgens RTL Nieuws duizenden euro's voor "omdat het relatief uniek is dat er op zo'n grote schaal burgerservicenummers worden verkocht."[4]

Direct na de berichtgeving van RTL Nieuws en de bekendmaking van de GGD GHOR volgt er een stroom van publieke verontwaardiging over het incident. De Autoriteit Persoonsgegevens (AP) meldt tegen RTL Nieuws dit "een zeer kwalijk en mogelijk ernstig datalek is" en dat de AP direct opheldering geëist heeft. De AP krijgt naar eigen zeggen "zeer veel telefoontjes" van verontruste mensen.[5] Om de vele vragen te kunnen beantwoorden, opent de GGD zelfs een speciale telefoonlijn waar burgers met vragen over de datadiefstal terecht kunnen. De datadiefstal leidt tot een uitvoerig debat in de Tweede Kamer.[6] Naar aanleiding van de datadiefstal kondigt Minister van VWS Huge de Jonge maatregelen aan om de kans op een datadiefstal te verkleinen.[7]

1 **https://www.rtlnieuws.nl/nieuws/nederland/artikel/5210644/handel-gegevens-nederlanders-ggd-systemen-database-coronit-hpzone** Laast bekeken op 15 mei 2021.
2 **https://ggdghor.nl/actueel-bericht/datadiefstal/** Laatst bekeken op 15 mei 2021.
3 **https://www.politie.nl/nieuws/2021/februari/15/03-update-6-mensen-aangehouden-voor-ggd-datadiefstal.html**
4 **https://www.rtlnieuws.nl/nieuws/nederland/artikel/5210644/handel-gegevens-nederlanders-ggd-systemen-database-coronit-hpzone** Laast bekeken op 15 mei 2021.
5 **https://www.rtlnieuws.nl/nieuws/nederland/artikel/5211077/privacywaakhond-zeer-veel-telefoontjes-over-datadiefstal-ggd** Laatst bekeken op 15 mei 2021.
6 **https://www.tweedekamer.nl/kamerstukken/plenaire_verslagen/detail/4d4207e2-7b5e-43a0-9957ccf71ca8017a#idf0704285** Laatst bekeken op 15 mei 2021.
7 **https://www.parool.nl/nederland/de-jonge-scherpere-controle-op-datadiefstal-ggd~b2ab7f51/** Laatst bekeken op 15 mei 2021.

PROBLEEMSTELLING

Cyberincidenten zoals de datadiefstal bij de GGD GHOR zijn een probleem dat in toenemende mate aandacht vraagt van organisaties. Aangezien verondersteld wordt dat cyberdreigingen (verder zullen) toenemen[8], moeten organisaties – van multinationals, mkb'ers tot zorginstellingen – zich hiertegen wapenen en dus investeren in cybersecurity. De vraag is echter hoe groot de cyberdreiging is en welke investering en maatregelen vanuit een kosten-baten perspectief gerechtvaardigd zijn.

De meeste organisaties bepalen hun maatregelen tegen cyberdreigingen op basis van een risicoanalyse waarbij de kans en impact van verschillende typen cyberincidenten worden ingeschat.[9] Om deze inschatting goed te kunnen maken, is feitelijk inzicht nodig in wat de impact is van cyberincidenten op verschillende dimensies zoals de financiën, bedrijfsvoering en/of reputatie van organisaties. In de wetenschappelijke literatuur is tot op heden nog maar beperkt aandacht besteed aan de (korte- en lange termijn) impact van cyberincidenten op organisaties.[10] Daarmee ontbreekt het feitelijke inzicht dat (ook voor zorg-) organisaties zo cruciaal is om geïnformeerde beslissingen te kunnen nemen over hoe om te gaan met cyberdreigingen en welke investering in cybersecurity proportioneel is.

In dit flitsonderzoek[11] willen we daarom achterhalen welke invloed de datadiefstal gehad heeft op een specifieke dimensie die relevant is voor organisaties in de zorgsector, namelijk het vertrouwen van patiënten in hun behandelaar en de zorginstelling. Deze dimensie heeft in recent empirisch onderzoek naar de impact van cyberincidenten op zorgorganisaties[12] niet of nauwelijks aandacht gekregen, terwijl in theorie de impact groot zou kunnen zijn. Immers zou een cyberincident er voor kunnen zorgen dat mensen zich minder snel laten behandelen door een bepaalde zorginstelling (bijvoorbeeld uit angst dat de zorginstelling getroffen wordt door een ransomware-aanval waardoor kritieke systemen uitvallen tijdens een behandeling) of minder vertrouwelijke informatie willen delen met hun behandelaar (bijvoorbeeld omdat ze vrezen dat gevoelige informatie over hun gezondheid in handen kan komen van derden).

Dit leidt tot de volgende onderzoeksvraag:

> **"Wat is de impact van de recente datadiefstal bij de GGD GHOR coronateststraten en bron- en contactonderzoek op het vertrouwen in de medewerkers van de GGD GHOR en de GGD GHOR als organisatie?"**

Om tot snelle disseminatie van de onderzoeksresultaten over te kunnen gaan, is besloten om de hoofdvraag te beantwoorden met behulp van een flitsonderzoek waarin de nadruk ligt op het verzamelen van empirische gegevens en deze voorzien van een eerste tentatieve duiding.

8 Een indicator is bijvoorbeeld de cijfers van het CBS: **https://www.cbs.nl/nl-nl/nieuws/2020/10/minder-traditionele-criminaliteit-meer-cybercrime**

9 Refsdal, A., Solhaug, B., & Stølen, K. (2015). Cyber-risk management. Springer, Cham.

10 Zie bijvoorbeeld: Falco, G., Eling, M., Jablanski, D., Weber, M., Miller, V., Gordon, L. A., ... & Maillart, T. (2019). Cyber risk research impeded by disciplinary barriers. Science, 366(6469), 1066-1069.

11 Een flitsonderzoek is een type onderzoek bedoeld om snel feiten te verzamelen ten behoeve van prangende maatschappelijke vraag of probleem. Op basis van deze feiten kan in de praktijk meer geïnformeerde besluitvorming plaatsvinden en door onderzoekers aanvullend onderzoek worden gedaan.

12 Bijvoorbeeld: Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., & Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. *NPJ digital medicine*, *2*(1), 1-7; Meisner, M. (2017). Financial consequences of cyber attacks leading to data breaches in healthcare sector. *Copernican Journal of Finance & Accounting*, *6*(3), 63-73.

PATIËNTVERTROUWEN

In dit flitsonderzoek sluiten we aan bij de wetenschappelijke literatuur over (het meten van) patiëntvertrouwen om inzicht te krijgen in de impact van de datadiefstal op het vertrouwen van mensen in de medewerkers of behandelaars van de coronateststraten en bron- en contactonderzoek en de GGD GHOR als zorginstelling.[13]

Patiëntvertrouwen kan volgens de wetenschappelijke literatuur gedefinieerd worden als het vertrouwen van een patiënt die in een kwetsbare situatie verkeert dat de behandelaar in het beste belang van de patiënt handelt.[14] In dit flitsonderzoek veronderstellen we dat er een verschil kan bestaan tussen het vertrouwen van patiënten in hun behandelaar en de zorginstelling waar de behandelaar werkzaam is.

Volgens de wetenschappelijke literatuur laat vertrouwen zich operationaliseren aan de hand van drie indicatoren: (1) vertrouwen in de deskundigheid en kwaliteit van de zorgverlener en zorginstelling, (2) behandelingstrouw en (3) vertrouwelijkheid tussen de informatie die uitgewisseld wordt tussen patiënt en zorgverlener. Tezamen geven deze indicatoren een beeld van het patiëntvertrouwen.

Het wetenschappelijk onderzoek naar patiëntvertrouwen heeft zich tot op heden met name gericht op de positieve effecten van (een hoog) patiëntvertrouwen. Onderzoek heeft bijvoorbeeld aangetoond dat een hoge mate van patiëntvertrouwen leidt tot het meer volgen van medische adviezen. Zo vond een onderzoek dat 62% van de personen in de groep met een hoge mate van patiëntvertrouwen altijd de voorgeschreven medicatie gebruikte en de medische adviezen opvolgde. Dit ten opzichte van slechts 14% van de personen in de groep met een laag niveau van patiëntvertrouwen.[15]

Ander onderzoek heeft laten zien dat een hoog patiëntvertrouwen een noodzakelijke rand-voorwaarde is voor de welwillendheid van patiënten om gevoelige informatie te delen met hun behandelaar.[16]

De vraag in hoeverre een cyberincident zoals een datadiefstal het patiëntvertrouwen negatief kan beïnvloeden (en daarmee de positieve effecten van patiëntvertrouwen teniet doet) kan op basis van het huidige wetenschappelijke onderzoek niet worden beantwoord. Dit flitsonderzoek levert een bijdrage om deze kennislacune te vullen.

13 Thom, D. H., Ribisl, K. M., Stewart, A. L., Luke, D. A., & The Stanford Trust Study Physicians. (1999). Further validation and reliability testing of the Trust in Physician Scale. ***Medical care***, 510-517; Thom, D. H., Hall, M. A., & Pawlson, L. G. (2004). Measuring patients' trust in physicians when assessing quality of care. ***Health affairs***, ***23***(4), 124-132.

14 Thom, D. H., Hall, M. A., & Pawlson, L. G. (2004). Measuring patients' trust in physicians when assessing quality of care. ***Health affairs***, ***23***(4), 124-132.

15 Thom, D. H., Ribisl, K. M., Stewart, A. L., Luke, D. A., & The Stanford Trust Study Physicians. (1999). Further validation and reliability testing of the Trust in Physician Scale. ***Medical care,*** 510-517.

16 Fuertes, J. N., Mislowack, A., Bennett, J., Paul, L., Gilbert, T. C., Fontan, G., & Boylan, L. S. (2007). The physician–patient working alliance. ***Patient education and counseling, 66***(1), 29-36.

METHODOLOGIE

Voor dit flitsonderzoek is een vragenlijst uitgezet onder een panel van I&O Research in Amsterdam. Hiertoe heeft I&O een steekproef getrokken die representatief is voor de Nederlandse bevolking. In totaal hebben 2031 mensen de vragenlijst beantwoord. De vragenlijst heeft uitgestaan in de periode februari-maart 2021.

RESULTATEN

De resultaten van het flitsonderzoek zijn onder te verdelen in vier categorieën: (1) vertrouwen in de deskundigheid van de GGD GHOR medewerkers en de GGD GHOR als zorginstelling, (2) behandelingstrouw of behandelingsbereidheid, (3) vertrouwelijkheid en het delen van informatie en (4) welke investering mensen zouden doen als ze directeur van de GGD GHOR zouden zijn.

Vertrouwen in deskundigheid

Een kleine meerderheid van de respondenten geeft aan dat datadiefstal niet leidt tot een vermindering van het vertrouwen in de deskundigheid van medewerkers (51,7%). Ook geeft de meerderheid aan dat de datadiefstal niet leidt tot een vermindering van het vertrouwen in de kwaliteit van de coronateststraten en het bron- en contactonderzoek (60,6%).

Desondanks geeft een significante groep (30%) aan minder vertrouwen te hebben in de deskundigheid van de medewerkers van de GGD GHOR. Bijna de helft van de respondenten (49,5%) geeft aan dat de datadiefstal het vertrouwen in de deskundigheid van de GGD-organisatie heeft geschaad. Tot slot geeft nog steeds een behoorlijke groep (19,3%) aan dat de datadiefstal tot een verminderd vertrouwen heeft geleid in de kwaliteit van de coronatesten en het bron- en contactonderzoek.

	Vragen	helemaal eens		eens		neutraal		oneens		helemaal oneens	
		%	n	%	n	%	n	%	n	%	
V1	De datadiefstal vermindert mijn vertrouwen in de deskundigheid van de medewerkers die de testen uitvoeren en het bron- en contactonderzoek doen.	8,3	441	21,7	372	18,3	785	38,7	265	13,0	
V2	De datadiefstal vermindert mijn vertrouwen in de deskundigheid van de GGD als organisatie	13,9	724	35,6	413	20,3	471	23,2	139	6,8	
V3	De datadiefstal vermindert mijn vertrouwen in de kwaliteit van de coronatesten en het bron en contactonderzoek	5,4	282	13,9	406	20,0	941	46,3	291	14,3	

Behandelingstrouw

Voor het merendeel van de respondenten heeft de datadiefstal geen negatieve invloed op de behandelingsbereidheid. Zo stelt het merendeel van de respondenten (65,9%) dat de datadiefstal er niet voor zorgt dat zij niet meer willen meewerken aan een coronatest of het bron- en contactonderzoek. Daarnaast geeft de meerderheid van de respondenten (64,7%) aan dat zij het testen op corona niet zouden uitstellen door de datadiefstal. Bovendien stelt een overgrote meerderheid (79,3%) dat de datadiefstal er niet toe leidt dat zij medische adviezen en voorschriften van de GGD GHOR niet meer zouden doen opvolgen.

Dat neemt overigens niet weg dat nog steeds een substantieel deel (18,5%) van de respondenten aangeeft dat de datadiefstal ervoor kan zorgen dat zij zich niet laat testen op corona of niet wil meewerken aan het bron- en contactonderzoek. Een iets hoger percentage (21,8%) geeft bovendien aan dat de datadiefstal kan leiden tot het uitstellen van het doen van een coronatest.

	Vragen	helemaal eens		eens		neutraal		oneens		helemaal oneens	
		%	n	%	n	%	n	%	n	%
V4	De datadiefstal kan ervoor zorgen dat ik wacht met mijzelf te laten testen op corona	7,1	299	14,7	273	13,4	878	43,2	436	21,5
V5	De datadiefstal kan er voor zorgen dat ik niet de medische adviezen en voorschriften over corona volg zoals aangegeven door de GGD	2,2	93	4,6	281	13,8	1097	54,0	514	25,3
V6	De datadiefstal kan ervoor zorgen dat ik mij niet laat testen op corona of niet wil meewerken aan bron- en contactonderzoek	5,7	260	12,8	316	15,6	902	44,4	437	21,5

Vertrouwelijkheid

Bijna de helft van de respondenten (45,9%) geeft aan dat de datadiefstal er voor kan zorgen dat zij minder persoonlijke (gevoelige) informatie zouden delen met een medewerker van de GGD GHOR teststraten of het bron- en contactonderzoek. Een iets groter percentage (49,1%) geeft zelfs aan dat de datadiefstal ervoor kan zorgen dat zij minder persoonlijke (gevoelige) informatie met de zorginstelling GGD GHOR zouden delen (denk hierbij bijvoorbeeld aan informatie over geslachtsziekten).

	Vragen	helemaal eens		eens		neutraal		oneens		helemaal oneens	
		%	n	%	n	%	n	%	n	%
V7	De datadiefstal kan er voor zorgen dat ik minder persoonlijke (gevoelige) informatie deel met een medewerker van de GGD teststraten of het bron- en contactonderzoek	12,3	683	33,6	450	22,2	463	22,8	186	9,2
V8	De datadiefstal kan er voor zorgen dat ik minder persoonlijke (gevoelige) informatie deel met de GGD als organisatie	14,0	713	35,1	417	20,5	444	21,9	171	8,4

Een kleinere groep (32%) stelt overigens dat de datadiefstal er niet voor zorgt dat zij minder vertrouwelijke informatie zou delen met een medewerker van de GGD teststraten of het bron- en contactonderzoek. Een gelijksoortig percentage (30,3%) geeft aan dat de datadiefstal er niet voor zorgt dat zij minder informatie zou delen met de GGD GHOR als organisatie.

Investeren in cybersecurity

Als laatste vraag hebben we de panelleden gevraagd om zich te verplaatsen in de rol van directeur GGD en te bepalen hoe zij (een denkbeeldig bedrag van) 1 miljoen euro aan extra middelen zouden willen inzetten. Door het stellen van deze vraag wilden we achterhalen hoe belangrijk de panelleden cybersecurity nu echt vinden na het lezen over de datadiefstal.[17] De precieze vraag was: "Stel, u bent directeur van de GGD en u krijgt van de Rijksoverheid 1 miljoen euro extra geld om naar eigen inzicht te besteden. En u moet een keuze maken uit een aantal mogelijkheden, wat kiest u?"

Waar zou u 1 miljoen euro extra geld aan willen besteden als u directeur van de GGD GHOR was?	
Uitbreiden testcapaciteit	13.96%
Verbeteren informatiebeveiliging en cybersecurity	49%
Meer opleidingen voor zorgpersoneel	10.04%
Beter kwaliteitstoezicht op het bron- en contactonderzoek en testen	18.77%
Anders, namelijk.	8.23%

17 Deze vraag is geïnspireerd op: Helsloot, I., Scholtens, A., Groenendaal, J., & Stapels, A. (2012). De Nederlandse burger nader verkend: nuchter mits geïnformeerd. Ministerie van BZK, Den Haag.

CONCLUSIES

De resultaten van dit flitsonderzoek laten een dubbel beeld zien:

- Het merendeel van de respondenten behoudt het vertrouwen in de medewerkers van de GGD GHOR en geeft aan dat de datadiefstal niet leidt tot een verminderde behandelingsbereidheid.

- Daarentegen zijn de respondenten kritisch op de GGD GHOR als organisatie: Bijna de helft van de respondenten verliest vertrouwen in de GGD GHOR als organisatie. Eenzelfde groep geeft aan dat de datadiefstal er (daardoor) voor kan zorgen dat er minder gevoelige informatie wordt gedeeld met de GGD GHOR.

Daarnaast is er een groep respondenten (ongeveer 20%) die uitgesproken negatief is over de invloed van de datadiefstal op het vertrouwen. Deze groep geeft aan dat de datadiefstal geleid heeft tot minder vertrouwen in de kwaliteit van coronatesten en het bron- en contactonderzoek. Een even grote groep geeft (daarom) aan dat de datadiefstal kan leiden tot een verminderde behandelingsbereidheid (dat wil zeggen uitstellen of niet laten testen en niet willen meewerken aan het bron- en contactonderzoek.

Uit dit flitsonderzoek blijkt tevens dat respondenten cybersecurity wel een belangrijk thema vinden voor de GGD GHOR. De helft van de respondenten zou namelijk als directeur van de GGD GHOR de 1 miljoen euro besteden aan het verbeteren van de informatiebeveiliging en cybersecurity. Ter vergelijking: het uitbreiden van de testcapaciteit wordt ‘maar’ door 13% van de respondenten gekozen.

Een belangrijke beperking van dit onderzoek is dat we in dit onderzoek met name intenties van respondenten hebben gemeten en niet hun daadwerkelijke gedrag. Ter illustratie: het feit dat 45,9% van de respondenten aangeeft dat de datadiefstal er voor kan zorgen dat zij minder persoonlijke (gevoelige) informatie delen met een medewerker van de GGD testraten of het bron- en contactonderzoek betekent niet dat zij dit ook daadwerkelijk doen. Nader (kwalitatief) onderzoek is daarom gewenst om te achterhalen in hoeverre een datadiefstal leidt tot een gedragsverandering.

Concluderend is het antwoord op de hoofdvraag van dit flitsonderzoek dat de datadiefstal vooral een negatieve invloed heeft (gehad) op het vertrouwen van mensen in de GGD GHOR organisatie en mensen (daardoor) minder snel geneigd zijn om gevoelige informatie te delen met de GGD GHOR.

Dit flitsonderzoek maakt volgens ons voldoende duidelijk dat mensen informatiebeveiliging binnen een organisatie zoals de GGD GHOR belangrijk vinden en dat hierin ook geïnvesteerd moet worden. Het laat tevens zien dat een majeur cyberincident kan leiden tot een verminderd vertrouwen in de organisatie. Hoewel meer onderzoek noodzakelijk is, zou dit er zelfs toe kunnen leiden dat mensen door een datadiefstal van coronagegevens minder snel geneigd zijn om informatie te delen met andere afdelingen binnen de GGD GHOR. Denk hierbij bijvoorbeeld aan het delen van informatie met de soapolikliniek. Dit maakt het voor een organisatie zoals de GGD GHOR dus belangrijk dat zij over de hele linie de informatiebeveiliging op orde hebben.

Alles bij elkaar hopen we daarmee dat dit flitsonderzoek een bijdrage levert aan geïnformeerde besluitvorming over cybersecurity investeringen binnen organisaties zoals de GGD GHOR en de gezondheidszorgsector in het algemeen.

APPENDIX: VRAGENLIJST FLITSONDERZOEK

Inleiding

Een paar weken geleden is bekend geworden dat enkele medewerkers van de GGD gevoelige gegevens gestolen hebben uit twee systemen: het systeem waarin medewerkers test- en vaccinatieafspraken registreren en het dossier waarin ze informatie uit bron- en contactonderzoeken vastleggen. Dit wordt ook wel een datadiefstal genoemd. De gestolen gegevens werden vervolgens verkocht op het internet aan andere criminelen die deze gegevens mogelijkerwijs kunnen gebruiken voor identiteitsfraude, waarbij bijvoorbeeld uw persoonlijke gegevens kunnen worden misbruikt om een lening aan te vragen. Of phishing-aanvallen, waarbij aanvallers u valse e-mails sturen en proberen om bijvoorbeeld uw bankgegevens te ontfutselen. Om de impact van dit cyberincident te kunnen meten vragen wij u de onderstaande stellingen te beantwoorden, met het bovenstaande voorbeeld in gedachte:

1. **De datadiefstal vermindert mijn vertrouwen in de deskundigheid* van de medewerkers die de testen uitvoeren en het bron- en contactonderzoek doen**

   Helemaal eens / eens / neutraal / oneens / helemaal oneens

   * Bij de deskundigheid van een medewerker kunt u aan de volgende dingen denken; de medewerker heeft goede (medische) kennis, is bekwaam in het uitvoeren van (medische) behandelingen, de medewerker luistert en communiceert goed met de patiënt, de medewerker geeft duidelijke voorlichting over de diagnose en behandel-mogelijkheden, de medewerker doet altijd wat het beste is voor de patiënt en de medewerker gaat professioneel om met de persoonlijke informatie van de patiënt.

2. **De datadiefstal vermindert mijn vertrouwen in de deskundigheid* van de GGD als organisatie**

   Helemaal eens / eens / neutraal / oneens / helemaal oneens

   *Bij de deskundigheid van de GGD kunt u aan de volgende dingen denken; de GGD heeft voldoende en deskundige medewerkers in dienst, de medewerkers heeft goede kwalitatieve faciliteiten voor medische zorg (bijvoorbeeld de nieuwste medische apparatuur), de GGD luistert en communiceert goed met de patiënt, de GGD doet altijd wat het beste is voor de patiënt en de GGD gaat professioneel om met de persoonlijke informatie van de patiënt.

3. **De datadiefstal vermindert mijn vertrouwen in de kwaliteit van de coronatesten en het bron en contactonderzoek**

   Helemaal eens / eens / neutraal / oneens / helemaal oneens

4. **De datadiefstal kan ervoor zorgen dat ik wacht met mijzelf te laten testen op corona**

   Helemaal eens / eens / neutraal / oneens / helemaal oneens

5. **De datadiefstal kan er voor zorgen dat ik niet de medische adviezen en voorschriften over corona volg zoals aangegeven door de GGD**

   Helemaal eens / eens / neutraal / oneens / helemaal oneens

6. **De datadiefstal kan ervoor zorgen dat ik mij niet laat testen op corona of niet wil meewerken aan bron- en contactonderzoek**

7. **De datadiefstal kan er voor zorgen dat ik minder persoonlijke (gevoelige) informatie deel met een medewerker van de GGD teststraten of het bron- en contactonderzoek**

   Helemaal eens / eens / neutraal / oneens / helemaal oneens

8. **De datadiefstal kan er voor zorgen dat ik minder persoonlijke (gevoelige) informatie deel met de GGD als organisatie**

   Helemaal eens / eens / neutraal / oneens / helemaal oneens

9. **Stel, u bent directeur van de GGD en u krijgt van de Rijksoverheid 1 miljoen euro extra geld om naar eigen inzicht te besteden. En u moet een keuze maken uit onderstaande mogelijkheden, wat kiest u?**

   a. Uitbreiden testcapaciteit
   b. Verbeteren informatiebeveiliging en cybersecurity om cyberincidenten te kunnen voorkomen
   c. Meer opleidingen voor zorgpersoneel
   d. Beter kwaliteitstoezicht op het bron- en contactonderzoek en testen
   e. Anders, namelijk.

Meer informatie

www.dehaagsehogeschool.nl

cybersecurity@hhs.nl

Johanna Westerdijkplein 75
2521 EN Den Haag

let's change
YOU. US. THE WORLD.