To: [redacted])[[redacted]@minvws.nl]
Cc: [redacted])[[redacted]@minvws.nl]; [redacted][[redacted]@minvws.nl]; [redacted].([redacted])[[redacted]@minvws.nl]; [redacted])[[redacted]@minvws.nl]; Functionaris Gegevensbescherming[[redacted]@ggdghor.nl]; Functionaris Gegevensbescherming[[redacted]@ggdghor.nl]; [redacted][[redacted]@ggdghor.nl]; [redacted][[redacted]@ggdghor.nl]
From: [redacted]
Sent: Sat 1/30/2021 1:50:12 PM
Subject: RE: Voorlopige bevindingen red teaming
Received: Sat 1/30/2021 1:50:17 PM

Beste [redacted]

Hartelijk dank voor de terugkoppeling. Naar aanleiding van de mondelinge terugkoppeling donderdag jl. zijn reeds de eerste acties in gang gezet. Deze zullen verder opgeschaald worden n.a.v. onderstaand overzicht. We houden contact over het vervolg hiervan.

Met vriendelijke groet,

[redacted]
[redacted]
GGD GHOR Nederland

E-mail: [redacted]@ggdghor.nl
Mobiel: [redacted]

Adres:
Zwarte Woud 2
3524 SJ Utrecht
www.ggdghor.nl

Van: [redacted]) <[redacted]@minvws.nl>
Verzonden: vrijdag 29 januari 2021 17:11
Aan: [redacted] | M&I/Partners <[redacted]@mxi.nl>; [redacted]@ggdghor.nl' <[redacted]@ggdghor.nl>
CC: [redacted]) <[redacted]@minvws.nl>; [redacted]) <[redacted]@minvws.nl>; [redacted]) <[redacted]@minvws.nl>; [redacted]) <[redacted]@minvws.nl>; Functionaris Gegevensbescherming <[redacted]@ggdghor.nl>
Onderwerp: Voorlopige bevindingen red teaming

Beste [redacted]

Eerder deze week hebben we afspraken gemaakt dat we ondersteuning bieden door red teaming en open source intelligence onderzoek te doen. Met je toestemming konden we al een aantal punten vinden. We blijven natuurlijk helpen met dit onderzoek.

Als uitgangspunten geldt dat we zoeken naar bevindingen die:

- Gevoelig zijn voor de beeldvorming rond GGD GHOR, de GGD'en of de bestrijding van COVID-19
- Gevoelig zijn vanuit de huidige media aandacht die speelt (we kijken naar impact en beschouwen de kans als 1)
- Het risicoprofiel van de GGD GHOR is hoog met actoren als activisten, journalisten en vreemde mogendheden die processen willen verstoren dan wel willen spioneren.

Als methodieken hebben we gebruik gemaakt van OSINT als offensievere aanvallen middels red teaming.

De bevindingen die we nu hebben zijn kort samengevat:

1. GGD Kennisnet is een website, die persoonsgegevens verwerkt. Op de website ontbreekt een privacy statement. Daarmee wordt niet voldaan aan de verplichtingen die uit de AVG vloeien.
2. GGD Kennis maakt het mogelijk om een account aan te maken op basis van een e-mailadres. Er wordt niet gecheckt of het adres daadwerkelijk bestaat of niet. Hiermee is dan ook niet zeker gesteld of iemand met een account überhaupt die persoon is. Het is mogelijk om als privepersoon te registreren. Daarbij is een mailadres te koppelen aan een organisatie, zoals een GGD of de GGD GHOR.
3. In aanvulling op het vorige punt kun je dus niet borgen dat persoonsgegevens alleen worden uitgewisseld tussen echte professionals. Of anders gezegd: het is niet uit te sluiten dat onbevoegden kennis nemen van persoonsgegevens van professionele medewerkers. Dat zou zeer wel een datalek kunnen zijn dat meldplichtig is. Het betreft hier immers duizenden accountgegevens.
4. Er is een mogelijkheid om je vrijelijk aan te melden voor besloten/semi-open groepen (afhankelijk van toestemming van een groepsbeheerder). De controle hierop schiet tekort, waardoor het mogelijk om bij vertrouwelijke gegevens te komen.
5. Je kunt in de verschillende groepen gegevens uploaden en daarmee desinformatie verspreiden. Door het niet controleren van deelnemers, kan dit heel schadelijk zijn.
6. Het is mogelijk om in bulk vertrouwelijke documenten te downloaden. Bijvoorbeeld een vaccinatiestrategie, die duidelijk als vertrouwelijk geldt. Er staan cijfers die niet stroken met de getallen die in de media circuleren, waardoor in de verkeerde handen dit onrust veroorzaakt. Denk ook aan beveiligingsgerelateerde informatie met details over transporten, procedures en meer. Of denk aan: Belscripts en werkinstructies fysieke vaccinatielocaties of plattegronden diverse vaccinatielocaties.
   Verder bijvoorbeeld werkinstructies, instructiefilms, technische beschrijvingen CoronIT of alle archieven en documenten van de projectgroep testfaciliteiten COVID-19;
7. Een ander voorbeeld van het vorige punt is het beschikbaar hebben van templates om mensen uit te nodigen voor vaccinatie. Het protocol zit zo in elkaar dat mensen niet worden gecontroleerd op rechtmatigheid van de brief. Met andere woorden het protocol laat fraude als mogelijkheid nadrukkelijk toe. Omdat achteraf dit ook niet meer is vast te stellen, is het denkbaar dat een dergelijke uitnodiging op de zwarte markt geld waard is. Het incident in Langsingerland maakt duidelijk dat de procedure van het zetten van de vaccinatie daadwerkelijk ook werkt, zoals beschreven.
8. Op sommige plaatsen slingeren inloggegevens van datalekken van jaren geleden. Sommige wachtwoorden werken nog. In het kader van kennisnet doet dit vermoeden dat wachtwoorden niet regelmatig worden vernieuwd.

We blijven natuurlijk verder kijken ook naar andere systemen en plekken, maar dit is belangrijk genoeg om vast te melden.

Harteljke groet,

5.1.2e
5.1.2e Programma RDO
Directie Informatiebeleid