To: 5.1.2e , 1.2. (5.1.2e)[5.1.2e @minvws.nl]
From: 5.1.2e , 5.1.2e . 5.1.2e . 5.1.2e - BD/NCSC
Sent: Mon 2/1/2021 3:34:40 PM
Subject: RE: Ernstige beveiligingsincident GGD Ghor Kennisnet website
Received: Mon 2/1/2021 3:34:49 PM

Dank.

Gegeven de gevoeligheid van onderstaande informatie zal ik je bericht niet verder doordelen (dus niet naar nctv doorsturen) tenzij je dat expliciet wel wilt gegeven de mh17 info.

Met vriendelijke groet,

5.1.2e 5.1.2e 5.1.2e

Van: 5.1.2e , 1.2. (5.1.2e) <5.1.2e @minvws.nl>
Datum: maandag 01 feb. 2021 4:14 PM
Aan: 5.1.2e , 5.1.2e . 5.1.2e . 1.2 - BD/NCSC <5.1.2e @ncsc.nl>
Onderwerp: FW: Ernstige beveiligingsincident GGD Ghor Kennisnet website

Ter info

Van: 5.1.2e , 5.1.2e . (5.1.2e)
Verzonden: maandag 1 februari 2021 16:07
Aan: 5.1.2e , 1.2. (5.1.2e) <5.1.2e @minvws.nl>
Onderwerp: FW: Ernstige beveiligingsincident GGD Ghor Kennisnet website

Beste 5.1.2e

Ik spring even bij 5.1.2e bij en pak dus even dit op.

Zie onderstaande mail.

Zou jij 5.1.2e willen bellen met de volgende boodschap:

1. Dit is ernstig en vraagt om directe maatregelen om de risico's weg te nemen (denk aan uitzetten);
2. Er zal onderzoek moeten plaatsvinden naar de aard van de documenten etc. op het gehele platform;
3. Indien de GGD geen actie onderneemt kan de minister niet anders dan hierin zelf actie ondernemen;
4. Op basis van de reeds gevonden documenten zullen wij bekijken wat dit betekent voor VWS en overige partijen binnen de rijksoverheid.

Kan jij hier mee uit voeten?

Groetjes 5.1.2e

5.1.2e 5.1.2e
5.1.2e PGB
5.1.2e

@ 5.1.2e @minvws.nl
5.1.2e

Voor het maken van een afspraak kan contact worden opgenomen met 5.1.2e
@ 5.1.2e @minvws.nl

5.1.2e

Van: 5.1.2e , 5.1.2e. (5.1.2e) < 5.1.2e @minvws.nl>
Verzonden: maandag 1 februari 2021 15:58
Aan: 5.1.2e , 5.1.2e. (5.1.2e) < 5.1.2e @minvws.nl>
Onderwerp: Ernstige beveiligingsincident GGD Ghor Kennisnet website

Beste 5.1.2e

VWS heeft onderzoek uitgevoerd naar kwetsbaarheden in de beveiliging bij de GGD-en. Aanleiding voor het onderzoek is het door RTL Nieuws gemelde beveiligingsincident.
Na het onderzoek is de vraag gerezen of er meer problemen zijn. Er is vervolgens verzocht door GGD GHOR aan VWS (programma Realisatie Digitale Ondersteuning) om onderzoek op het gebied van open bronnen en aanvallen, die niet systemen direct schaden uit te voeren.

Tijdens het onderzoek is de website kennisnet van GGD GHOR in beeld gekomen als plaats waar veel verschillende documenten en personen te vinden zouden zijn. Het blijkt dat iedereen een account kan aanmaken met een al dan niet bestaand e-mailadres. Met ingevoerde gegevens is het mogelijk om bij besloten groepen te komen. In veel groepen worden mensen zonder nadere screening of contact toegelaten.

De gevonden kwetsbaarheden zijn dusdanig ernstig dan wij adviseren om direct actie te ondernemen en de website direct offline te halen.

Enkele gevonden kwetsbaarheden:

Inzake COVID-19 testen/vaccinaties:

- Bevat logistieke details aangaande beveiliging transporten, locaties (wanneer opschakelen, hoeveel personeel etc.)
- Bevat vertrouwelijke presentaties en gespreksverslagen inzake vaccinatiestrategie (incl. niet gepubliceerde cijfers beschikbare vaccins)
- Standaardbrieven in template vorm (o.a. uitnodigingen, afspraakbevestigingen) waarmee zowel 'voorgedrongen' kan worden alsook het proces ernstig verstoord kan worden
- Contactgegevens van coördinatoren
- Bevat (interne) handleidingen en (nood)werkinstructies o.a. over CoronIT, HPZone, zoeken van persoonsgegevens etc.
- Bevat procesinformatie waarmee processen rond vaccinatie te manipuleren zijn (o.a. belscripts en Q&As)

Inzake MH-17:

- Diverse docs "SITRAP" en "Omgevingsanalyse" voor het Departementaal Crisiscentrum (DCC) van VWS:
- Departementaal vertrouwelijk
- Namen van betrokken ambtenaren ("aan:")
- Namen van opstellers (politie, VWS, Veiligheidsregio)
- Gebruikte zoektermen / bronnen
- Info in documenten onder kopjes als "schadebeperking", "betekenisgeving", "relevante actoren", etc.
- Naam van opsteller van documenten is persoon die uit gerelateerde WOB-verzoeken is weggelakt 5.1.2e BD/DRD/NCC/ECO, 06-20252612 (in WOB-verzoeken aangeduid als 5.1.2e

GGD-GHOR Kennisnet kwetsbaarheden algemeen:

- Geen verificatie van accounts
- Te benaderen zowel als buitenstaander met aan te maken account als met gelekte inloggegevens van bestaand personeel
- Met gelekte inloggegevens is het mogelijk in te loggen bij digvi.ggdghorkennisnet.nl, het Digitaal Veldinstrument Toezicht Kinderopvang, waarmee inspecties kunnen worden gedaan.
- Te misbruiken door implanteren foutieve informatie omtrent werkprocessen
- Kan reeds langdurig geïnfiltreerd zijn i.v.m. aanwezige gevoelige informatie (bijvoorbeeld rondom MH-17) beschikbaar op het platform
- Met 20k+ ongeverifieerde gebruikers niet eenvoudig te zuiveren/vervangen als platform
- Laatste update platform 2017

Afgelopen vrijdag 29 januari 2021 zijn de CISO, de Functionaris Gegevensbescherming en ons reguliere aanspreekpunt bij de GGD Ghor per mail geïnformeerd dat er sprake is van een datalek. Hierin stonden bovenstaande kwetsbaarheden zonder de MH17 (die waren toen nog niet bekend). Hierop is geen reactie gekomen anders dan een standaard ontvangstbevestiging van het bericht. Vandaag is gerappelleerd dat de deadline van 72 uur, die in de AVG wordt genoemd voor het melden van een lek, in het geding komt.
Daarnaast is ook gemeld dat er vertrouwelijke documenten te vinden zijn, waarin het lekken van namen zelfs een risico kan zijn (bijvoorbeeld in het geval van de MH17).

Bij het onderzoek is tevens gebleken dat er een probleem in de rol van 5.1.2e 5.1.2e zit. 5.1.2e 5.1.2e 5.1.2e 5.1.2e
Hierdoor ontstaat de onwenselijke situatie dat 5.1.2e Dit is 5.1.2e

Het lijkt onvermijdelijk dat Kennisnet met alle beveiligingsproblemen per direct wordt uitgeschakeld. Daarnaast moet een inventarisatie worden gemaakt van de echt noodzakelijke informatie en waar deze alsnog toegankelijk kan worden gemaakt.

5.1.2e 5.1.2e 5.1.2e en ikzelf zijn beschikbaar om toelichting te geven.

Vriendelijke groeten,

5.1.2e
5.1.2e 5.1.2e 5.1.2e
5.1.2e
Ministerie van Volksgezondheid, Welzijn en Sport
5.1.2e @minvws.nl | 5.1.2e
Parnassusplein 5 | 2511 VX | Den Haag
Postbus 20350 | 2500 EJ | Den Haag

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

Ministerie van Justitie en Veiligheid

Ministry of Justice and Security