To: (10)(2e) [(10)(2e)@rivm.nl]; (10)(2e) [(10)(2e)@rivm.nl]; (10)(2e) (10)(2e) [(10)(2e)@rivm.nl]; (10)(2e) [(10)(2e)@rivm.nl]
Cc: Informatiebeveiliging[(10)(2e)@rivm.nl]
From: (10)(2e)
Sent: Tue 6/9/2020 11:36:31 AM
Subject: RE: belangrijke overweging
Received: Tue 6/9/2020 11:36:32 AM

Dank (10)(2e)

@(10)(2e) En dan inderdaad zeker gelet op de perikelen rondom infectieradar. Je kunt er volgens mij namelijk vanuit gaan dat dit onderzoek vanuit verschillende hoek "getarged" gaat worden. Een lek in de beveiliging is dan doorgaans vrij snel gevonden.

Dat geen gebruik wordt gemaakt van Formdesk of dat een link met cijfers en letters wordt gebruikt geeft bijvoorbeeld niet de vereiste waarborgen. Taz van de link zou bijvoorbeeld doorlopend getest moeten worden of deze link kan worden misbruikt.

Kortom: gelet op de omvang van het onderzoek, de mediagevoeligheid en uiteraard vooral voor de bescherming van de deelnemers zou ik zeker adviseren om alle mogelijke maatregelen te treffen.

In een eerder stadium heb ik bijvoorbeeld begrepen dat R2E op verschillend niveau (op het systeem) encryptie zou kunnen aanbieden. IK kan mij voorstellen dat je bijvoorbeeld wilt checken of encryptie inmiddels is geïmplementeerd.

Hartelijke groet,
(10)(2e)

From: (10)(2e) <(10)(2e)@rivm.nl>
Sent: dinsdag 9 juni 2020 12:52
To: (10)(2e) <(10)(2e)@rivm.nl>; (10)(2e) <(10)(2e)@rivm.nl>; (10)(2e) <(10)(2e)@rivm.nl>; (10)(2e) <(10)(2e)@rivm.nl>
Cc: Informatiebeveiliging <(10)(2e)@rivm.nl>
Subject: RE: belangrijke overweging

Hallo (10)(2e) en andere collega's,

Volgens mij heeft (10)(2e) als onze informatiemanager ook contact gehad met Research2Evolve in het kader van een Quickscan BIO.
(10)(2e) denk jij dat het zinvol is om dit bedrijf nader te onderzoeken?

Groet, (10)(2e)

Van: (10)(2e) <(10)(2e)@rivm.nl>
Datum: 9 juni 2020 om 12:10:23 CEST
Aan: (10)(2e) <(10)(2e)@rivm.nl>, (10)(2e) <(10)(2e)@rivm.nl>, (10)(2e) <(10)(2e)@rivm.nl>
CC: Informatiebeveiliging <(10)(2e)@rivm.nl>
Onderwerp: RE: belangrijke overweging

Beste (10)(2e) en (10)(2e)
Ik heb net (10)(2e) van het onderzoeksbureau gesproken.
Bij het vragenlijstonderzoek zijn de links versleuteld met letters en cijfers. Zij maken geen gebruik van formdesk.
Informatiebeveiliging heeft meen ik ook al een 'plaat' van dit onderzoek gemaakt. En was meen ik 'goedgekeurd'.

Verder gaf (10)(2e) aan dat je natuurlijk nooit 100% garantie kan geven dat je gehackt wordt, maar dat er wel alles aan gedaan wordt om dat te voorkomen.

Is dit voldoende info of moeten we hier nog wat mee?

Groetjes (10)(2e)
(10)(2e)

---

(10)(2e) - Afdeling Voeding en Gezondheid
http://wateetnederland.nl

(10)(2e) - Corona Gedragsunit
https://www.rivm.nl/coronavirus-covid-19/onderzoek/gedrag

RIVM
Adres: Postbus 1, 3720 BA Bilthoven
tel: +31 (10)(2e)
e-mail: (10)(2e) @rivm.nl
twitter: @ (10)(2e)

From: (10)(2e) < (10)(2e) @rivm.nl>
Sent: dinsdag 9 juni 2020 07:59
To: (10)(2e) < (10)(2e) @rivm.nl>; (10)(2e) < (10)(2e) @rivm.nl>
Cc: Informatiebeveiliging < (10)(2e) @rivm.nl>
Subject: belangrijke overweging
Importance: High

Goedemorgen (10)(2e) en (10)(2e)

Waarschijnlijk zijn jullie bekend met de perikelen rondom infectieradar.
In navolging daarvan het advies om voor het gedragsonderzoek goed na te gaan of de beveiliging nog altijd goed geregeld is bij bijvoorbeeld verwerker R2E.

Gezien de omvang van het onderzoek bestaat uiteraard de kans dat ook dit onderzoek nader wordt bekeken door journalisten/hackers.

Laat gerust weten mochten jullie vragen hebben.

Met vriendelijke groet,

(10)(2e) (10)(2e) | (10)(2e)
RIVM
Stafeenheid Finance, Compliance en Control (FCC)

Antonie van Leeuwenhoeklaan 9 | 3721 MA Bilthoven
M: (10)(2e)