Inventarislijst – bijlage 2

No.	Te openbaren informatie	Datum	Beschrijving	Beoordeling	Grond
1	mail - [NCSC-NL 195101] Verzoek tot ondersteuning en coördinatie	1 oktober 2022	Antwoord van NCSC ontvangstbevestiging verzoek aan NCSC voor ondersteuning en coördinatie	Deels openbaar	5.1.2.e
2	mail - Melding piket ID-ware	1 oktober 2022	Email over de eerste signalen van de hack van piketdienst rijksoverheid	Deels openbaar	5.1.2.e 5.1.2.f 5.1.2.i
3	mail – woordvoeringslijn, eerste versie	1 oktober 2022	Eerste versie woordvoeringslijn	Deels openbaar	5.1.2.e
4	20221002 Communicatievoorstel ID-ware v0.1	2 oktober 2022	In dit communicatievoorstel worden 3 scenario's geschetst.	Deels openbaar	5.1.2.i/5.2.1
5	mail - FW Aanvullende vragen m.b.t. hack ID-Ware	2 oktober 2022	Aanvullende vragen van de tweede kamer aan CISO Rijk rondom de hack op ID-ware	Deels openbaar	5.1.2.e
6	Verslag integraal overleg casus ID Ware 03-10-2022	3 oktober 2022	Verslag van het integrale overleg met daarin opgenomen de beeldvorming, Oordeelsvorming en Besluitvorming	Deels openbaar	5.1.2.e 5.1.2.f 5.1.2.h
--	FW: Update Tweede Kamer and ID-ware	6 oktober 2022	Prelimenary analysis ID-ware	Niet openbaar	5.1.2.f
7	Mail - RE: Opzet brief ID-ware 0.1 rev aj.docx	6 oktober 2022	Mailwisseling over de opzet kamerbrief	Deels openbaar	5.1.2.e 5.1.2.f 5.1.2.h
8	intern - duiding mediaberichtgeving	7 oktober 2022	Document met duiding mediaberichtgeving o[gesteld door woordvoering	Deels openbaar	5.1.2.f
9	intern - IDW_IT-Incident-PR-statement_NL_01_07.10.2022	7 oktober 2022	Opgesteld door ID-ware Incident statement (4d. behorende bij doc.nr. 3 Duiding mediaberichtgeving)	Deels openbaar	nvt
10	mail - Hack ID-ware	7 oktober 2022	Interne ter kennisgeving	Deels openbaar	5.1.2.e
11	mail - Rijksoverheid TLPAMBER Berichtgeving rondom de hack bij ID-ware	7 oktober 2022	Doelgroepbericht NCSC [TLP: AMBER]	Openbaar	nvt
12	mail - RE Rijkspas	7 oktober 2022	Interne vragen over inrichting	Deels openbaar	5.1.2.e 5.1.2.i
13	mail - RE Communicatie	7 oktober 2022	bevestiging NCTV over betrokkenheid	Deels openbaar	5.1.2.e
14	mail - RE QA Hack	7 oktober 2022	Interne vragen over inrichting	Deels openbaar	5.1.2.e 5.1.2.i
15	Aantekeningen overleg ransomware aanval op ID-ware - 9 okt 2100	9 oktober 2022	Overleg tussen de betrokken partijen binnen de crisisorganisatie ten tijde van de afhandeling van het incident. Dit document bestond in meerdere versies, bijgewerkt vanaf 2 oktober	Deels openbaar	5.1.2.b 5.1.2.e 5.1.2.f 5.1.2.i
16	Mail - RE: Bijgewerkte tijdlijn	10 oktober 2022	Begeleidende email over de bijgewerkte tijdslijn	Deels openbaar	5.1.2.e
17	intern - Factsheet en tijdlijn	10 oktober 2022	Factsheet en tijdlijn ID-ware hack t.b.v. mondelinge vragenuur	Deels openbaar	5.1.2.f
18	mail - RE Kamerbrief update hack bij ID-ware - Tweede Kamer	10 november 2022	Interne vragen over afstemming	Deels openbaar	5.1.2.e 5.1.2.i/5.2.1

19	Mail - RE: Update ransomware-aanval ID-ware	20 oktober 2022	Update intern CIO Rijk	Deels openbaar	5.1.2.e 5.1.2.f
20	mail - RE Vragen Stas ransomware-aanval ID-ware	25 oktober 2022	Mailwisseling over vragen van de staatssecretaris	Deels openbaar	5.1.2.e Buiten reikwijdte
21	mail - RE Debat 2 november - stasBZK	27 oktober 2022	Interne afstemming Q&A en schema debat	Deels openbaar	5.1.2.e 5.1.2.i/5.2.1 Buiten reikwijdte
22	mail - RE Status ID-ware en uitwerking evaluatiesessie 1 november	11 november 2022	Uitwerking van de evaluatiesessie op de afhandeling van het incident	Deels openbaar	5.1.2.e
23	Mail - RE: Evaluatie incident ID-ware	27 oktober	Mailwisseling met afstemming over vergaderdata	Deels openbaar	5.1.2.e
24	221101 evaluatie ID-ware v0.1	1 november 2022	Dit document geeft de belangrijkste noties, bevindingen en aanbevelingen tot vervolg weer op 4 onderdelen: 'incident'; 'coördinatie'; 'communicatie', 'verder onderzoeken en verbeterpunten'.	Deels openbaar	5.1.2.e 5.1.2.b 5.1.2.f
25	mail - FW Vragen FD over hack ID-Ware	2 november 2022	Reactie op vragen van het FD	Deels openbaar	5.1.2.e 5.1.2.i/5.2.1
26	brief - ID ware Reactie inzake Hackaanval Rijkpassen	4 november 2022	Reactie van ID-ware met excuses, verklaring en uitleg hoe de hack heeft kunnen plaatsvinden	Deels openbaar	5.1.2.e 5.1.2.f 5.1.2.h
27	mail - 221101 evaluatie ID-ware v0.1	24 november 2022	Emailwisseling rondom de resultaten van de evaluatie op het incident betreffende de hack op ID-ware	Deels openbaar	5.1.2.e Buiten reikwijdte
28	mail - RE Via e-mail verzenden 02. Kamerbrief hack bij ID-ware.docx	31 oktober 2022	Begeleidende brief voor de kamerbrief over de update hack bij ID-ware van 10 november	Deels openbaar	5.1.2.e Buiten reikwijdte
29	signal – Berichten	1 oktober – 20 oktober 2022	Signalberichten van het crisisteam bij de afhandeling van het incident	Deels openbaar	5.1.2.b 5.1.2.e 5.1.2.f Buiten reikwijdte
30	intern - Oplegger Mondelinge Vraag		Mondelinge vraag van het lid: Dekker-Abdulaziz (D66) aan de staatssecretaris voor Koninkrijksrelaties en Digitalisering over het hack bij ID-ware/de rijkspas (n.a.v. Kamerbrief op vrijdag 7 oktober; opgepakt door verschillende media)	Deels openbaar	5.1.2.e
--	intern – Spreektekst		Spreektekst ID-ware t.b.v. mondelinge vragenuur	Niet openbaar	5.1.2.i
31	Intern – Mediaverzicht data toegangspassen-3.pdf		Overzicht van alle berichten in de media	Openbaar	nvt

Reeds openbare documenten	Datum publicatie	Beschrijving	Lokatie
Beslisnota bij Kamerbrief Hack ID-ware	6 oktober 2022	In een beslisnota staat achtergrondinformatie die bewindspersonen gebruiken bij de besluitvorming over een Kamerstuk.	Beslisnota bij Kamerbrief hack ID-ware | Beleidsnota | Rijksoverheid.nl
Kamerbrief hack ID-ware	7 oktober 2022	Staatssecretaris Van Huffelen (Koninkrijksrelaties en Digitalisering) informeert de Tweede Kamer over de recente ontwikkelingen rondom de hack op een leverancier voor de uitgifte van Rijkspassen. De Eerste Kamer heeft eenzelfde brief gekregen.	Kamerbrief hack ID-ware | Kamerstuk | Rijksoverheid.nl
Beslisnota bij Kamerbrief over update hack bij ID-ware	9 november 2022	In een beslisnota staat achtergrondinformatie die bewindspersonen gebruiken bij de besluitvorming over een Kamerstuk.	Beslisnota bij Kamerbrief over update hack bij ID-ware | Beleidsnota | Rijksoverheid.nl
Kamerbrief over update hack bij ID-ware	10 november	Staatssecretaris Van Huffelen (Koninkrijksrelaties en Digitalisering) informeert de Tweede Kamer over het afronden van het onderzoek rondom de hack op ID-ware. ID-ware is een bedrijf dat diensten levert voor de Rijkspasvoorziening en voor beheer van toegangspassen voor de Eerste Kamer en Tweede Kamer. De Eerste Kamer heeft eenzelfde brief gekregen.	Kamerbrief over update hack bij ID-ware | Kamerstuk | Rijksoverheid.nl

1

5.1.2.e

Van: cert@ncsc.nl
Verzonden: zaterdag 1 oktober 2022 12:39
Aan: 5.1.2.e
Onderwerp: [NCSC-NL #195101] Verzoek tot ondersteuning en coordinatie

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

Beste 5.1.2.e,

hierbij bevestiging dat het verzoek in goede aarde ontvangen is, we nemen spoedig contact op over de vervolgstappen.

Met vriendelijke groet,
5.1.2.e

Nationaal Cyber Security Centrum
Postbus 117 | 2501 CC | Den Haag | www.ncsc.nl
E cert@ncsc.nl
T +31 070 751 55 55 (algemeen)
PGP 486E F5E3 82B5 5BCA 1C66 A923 1CA9 5AAC 3F66 2B80
Bezoekadres:
Turfmarkt 147 | 2511 DP | Den Haag

-----BEGIN PGP SIGNATURE-----
Version: Encryption Desktop 10.4.2 (Build 1298)
Charset: utf-8

wsDVAwUBYzgYyhypWqw/ZiuAAQqu5wwArM9emrGi6hteM+Bi5sJttD4qCF5Yu8lN
2K3pHz8NqFleBHj7r78aeCb8XUdmJ1gbUSMPE0mVBmxcIGff4UKkGIU9Va/PUg53
y7MRzIzhry8mrzqGBsiEO6MBJx+lHuoLO5ApFxVErtk7Nyg+ypw8qSbWNlyvEx49
gD6jPH+0Ht5ZcWLff1fUJUuBy90K6dQBZ8jrU9iXAVd5V6d5NfkU8ohZJILQfs24
KeEbkIdprt4DUvDjc5JNoqapWIKWjAPxwIfI0W7H1kLGg579CCnxe3xXJUk9UhUP
Ta3ucGQUyMQnUIL/g0GWFL+iBLdAfPqgu7/oPS2pI3PGFN1j35QOQ7+A4FOa3ZQ4
5Ce/V6fPBpOD/USS9hiS4AE8aRhKG1CWJbVcv580rUKjLxHoSIvHQQ4HIwBjcmhg
LY7zjYLSAWI649n8vV3LyZbYTc60YiisjHpvY4gokC0Q89G6YF7cBvzsBOG+nTY4
Hk9l4uEnvm3S6L0KiQjjZLswstK7czC9
=nNRF
-----END PGP SIGNATURE-----

2

5.1.2.e

Van: 5.1.2.e
Verzonden: zaterdag 1 oktober 2022 13:34
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: Melding piket ID-Ware

Beste 5.1.2.e ,

Ik heb vanmorgen overleg gehad met de BVA's Eerste en Tweede Kamer over een melding van ID-Ware dat zij een ransomware aanval hebben gehad en hebben geconstateerd dat er een grrot aantal bestanden zijn geëxfiltreerd. ID-Ware voert diensteverlening uit rond de Rijkspas, voor de EK en TK als SAAS dienst (en beheren dus ook de gegevens) en voor Rijkspas Rijksoverheid (gegevens in beheer van Rijkspas). CIO Rijk heeft regie genomen namens EK, TK en Rijksoverheid. Voor de operationele coördinatie heb ik NCSC ingeschakeld.

Situatie
Op 21 september werd bekend dat ID Ware een aanval heeft gehad op hun systemen en er mogelijk sprake zou kunnen zijn van een datalek. Er is toen al contact geweest tussen TK en CIO Rijk. ID-Ware heeft 5.1.2.f ingeschakeld en verwachtte afgelopen week met een rapportage te komen. In plaats daarvan ontvin de TK afgelopen donderdag een brief waarin duidelijk werd dat het om een ransomware-aanval ging, waarbij ook bestanden zijn geëxfiltreerd. Op darkweb is een lijst met bestandsnamen gepubliceerd, waarna nu onderzoek wordt gedaan. Onduidelijk is nog of deze bestanden ook klantgegevens bevatten. Dat onderzoek loopt nog. Er is nog geen aangifte gedaan. NCSC was nog niet betrokken.

Na overleg met CISO TK heb ik contact gezocht met NCSC. Zij hadden wel al signalen gezien, maar nog geen melding gekregen. Vanmorgen heb ik overleg gehad met BVA's EK en TK en hebben we afgesproken dat CIO Rijk de regie neemt. Hierna heb ik contact gehad met NCSC en hun ondersteuning gevraagd om met ID-Ware, 5.1.2.f en Politie samen te werken om de impact te onderzoeken en de juiste opvolging te geven. Vanmiddag is er weer een overleg tussen EK, TK en CIO Rijk en, als er meer info is met NCSC.

Voor EK en TK is de mogelijke impact het grootsts: naast een mogelijk datalek die medewerkers en leden van EK en TK raakt, 5.1.2.e . Voor de Rijkspas Rijksoverheid lijkt de impact tot nog toe beperkt (als het goed is geen datalek), dit moet nog verder worden uitgezocht. Als er meer over bekend is laat ik het weten.

Groet,

5.1.2.f

5.1.2.e
5.1.2.e
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Directie CIO Rijk | DG Overheidsorganisatie
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20011 | 2500 AE | Den Haag
e-mail: 5.1.2.e @minbzk.nl
telefoon secretariaat: 5.1.2.e | mobiel: 5.1.2.e

5.1.2.e

Van: 5.1.2.e
Verzonden: zaterdag 1 oktober 2022 16:28
Aan: 5.1.2.e
Onderwerp: FW: Melding piket ID-Ware

Ha 5.1.2.e,

Ter info.

Groet,

5.1.2.e

Van: 5.1.2.e
Verzonden: zaterdag 1 oktober 2022 13:34
Aan: 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>
CC: 5.1.2.e <5.1.2.e @minbzk.nl>
Onderwerp: Melding piket ID-Ware

Beste 5.1.2.e,

Ik heb vanmorgen overleg gehad met de BVA's Eerste en Tweede Kamer over een melding van ID-Ware dat zij een ransomware aanval hebben gehad en hebben geconstateerd dat er een grrot aantal bestanden zijn geëxfiltreerd. ID-Ware voert diensteverlening uit rond de Rijkspas, voor de EK en TK als SAAS dienst (en beheren dus ook de gegevens) en voor Rijkspas Rijksoverheid (gegevens in beheer van Rijkspas). CIO Rijk heeft regie genomen namens EK, TK en Rijksoverheid. Voor de operationele coördinatie heb ik NCSC ingeschakeld.

Situatie
Op 21 september werd bekend dat ID Ware een aanval heeft gehad op hun systemen en er mogelijk sprake zou kunnen zijn van een datalek. Er is toen al contact geweest tussen TK en CIO Rijk. ID-Ware heeft 5.1.2.f ingeschakeld en verwachtte afgelopen week met een rapportage te komen. In plaats daarvan ontvin de TK afgelopen donderdag een brief waarin duidelijk werd dat het om een ransomware-aanval ging, waarbij ook bestanden zijn geëxfiltreerd. Op darkweb is een lijst met bestandsnamen gepubliceerd, waarna nu onderzoek wordt gedaan. Onduidelijk is nog of deze bestanden ook klantgegevens bevatten. Dat onderzoek loopt nog. Er is nog geen aangifte gedaan. NCSC was nog niet betrokken.

Na overleg met CISO TK heb ik contact gezocht met NCSC. Zij hadden wel al signalen gezien, maar nog geen melding gekregen. Vanmorgen heb ik overleg gehad met BVA's EK en TK en hebben we afgesproken dat CIO Rijk de regie neemt. Hierna heb ik contact gehad met NCSC en hun ondersteuning gevraagd om met ID-Ware, 5.1.2.f en Politie samen te werken om de impact te onderzoeken en de juiste opvolging te geven. Vanmiddag is er weer een overleg tussen EK, TK en CIO Rijk en, als er meer info is met NCSC.

Voor EK en TK is de mogelijke impact het grootsts: naast een mogelijk datalek die medewerkers en leden van EK en TK raakt, 5.1.2.e. Voor de Rijkspas Rijksoverheid lijkt de impact tot nog toe beperkt (als het goed is geen datalek), dit moet nog verder worden uitgezocht. Als er meer over bekend is laat ik het weten.

Groet,

5.1.2.e

5.1.2.e

5.1.2.e

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Directie CIO Rijk | DG Overheidsorganisatie
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20011 | 2500 AE | Den Haag

e-mail: 5.1.2.e @minbzk.nl
telefoon secretariaat: 5.1.2.e | mobiel: 5.1.2.e

5.1.2.e

Van: 5.1.2.e
Verzonden: zondag 2 oktober 2022 08:44
Aan: Huffelen, Alexandra van
Onderwerp: FW: Melding piket ID-Ware

Excuus, verkeerde mailadres

Van: 5.1.2.e <5.1.2.e @minbzk.nl>
Verzonden: zaterdag 1 oktober 2022 17:39
Aan: Huffelen, AC (Alexandra) van (STAS) <5.1.2.e @minfin.nl>
CC: 5.1.2.e <5.1.2.e @minbzk.nl>
Onderwerp: FW: Melding piket ID-Ware

Beste Alexandra,

Op verzoek van 5.1.2.e informeer ik je hieronder over een incident bij een leverancier van de Eerste Kamer, Tweede Kamer en Rijksoverheid voor de Rijkspas. Er is nog weinig informatie, maar onderzoek loopt. Als er meer informatie komt informeren we je zonodig; en anders in het PO. Er is een woordvoeringslijn gedeeld.

Met vriendelijke groet,

5.1.2.e

5.1.2.e

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Directie CIO Rijk | DG Digitalisering en Overheidsorganisatie
Turfmarkt 147 | 2511 DP | Den Haag
e-mail: 5.1.2.e @minbzk.nl
mobiel: 5.1.2.e | telefoon secretariaat: 5.1.2.e

Van: 5.1.2.e <5.1.2.e @minbzk.nl>
Datum: zaterdag 01 okt. 2022 4:28 PM
Aan: 5.1.2.e <5.1.2.e @minbzk.nl>
Onderwerp: FW: Melding piket ID-Ware

Ha 5.1.2.e,

Ter info.

5.1.2.e,

5.1.2.e

Van: 5.1.2.e
Verzonden: zaterdag 1 oktober 2022 13:34
Aan: 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>
CC: 5.1.2.e <5.1.2.e @minbzk.nl>
Onderwerp: Melding piket ID-Ware

Beste 5.1.2.e ,

Ik heb vanmorgen overleg gehad met de BVA's Eerste en Tweede Kamer over een melding van ID-Ware dat zij een ransomware aanval hebben gehad en hebben geconstateerd dat er een grrot aantal bestanden zijn geëxfiltreerd. ID-Ware voert diensteverlening uit rond de Rijkspas, voor de EK en TK als SAAS dienst (en beheren dus ook de gegevens) en voor Rijkspas Rijksoverheid (gegevens in beheer van Rijkspas). CIO Rijk heeft regie genomen namens EK, TK en Rijksoverheid. Voor de operationele coördinatie heb ik NCSC ingeschakeld.

Situatie
Op 21 september werd bekend dat ID Ware een aanval heeft gehad op hun systemen en er mogelijk sprake zou kunnen zijn van een datalek. Er is toen al contact geweest tussen TK en CIO Rijk. ID-Ware heeft 5.1.2.f ingeschakeld en verwachtte afgelopen week met een rapportage te komen. In plaats daarvan ontvin de TK afgelopen donderdag een brief waarin duidelijk werd dat het om een ransomware-aanval ging, waarbij ook bestanden zijn geëxfiltreerd. Op darkweb is een lijst met bestandsnamen gepubliceerd, waarna nu onderzoek wordt gedaan. Onduidelijk is nog of deze bestanden ook klantgegevens bevatten. Dat onderzoek loopt nog. Er is nog geen aangifte gedaan. NCSC was nog niet betrokken.

Na overleg met CISO TK heb ik contact gezocht met NCSC. Zij hadden wel al signalen gezien, maar nog geen melding gekregen. Vanmorgen heb ik overleg gehad met BVA's EK en TK en hebben we afgesproken dat CIO Rijk de regie neemt. Hierna heb ik contact gehad met NCSC en hun ondersteuning gevraagd om met ID-Ware, 5.1.2.f en Politie samen te werken om de impact te onderzoeken en de juiste opvolging te geven. Vanmiddag is er weer een overleg tussen EK, TK en CIO Rijk en, als er meer info is met NCSC.

Voor EK en TK is de mogelijke impact het grootsts: naast een mogelijk datalek die medewerkers en leden van EK en TK raakt, 5.1.2.e . Voor de Rijkspas Rijksoverheid lijkt de impact tot nog toe beperkt (als het goed is geen datalek), dit moet nog verder worden uitgezocht. Als er meer over bekend is laat ik het weten.

Groet,

5.1.2.e

5.1.2.e

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Directie CIO Rijk | DG Overheidsorganisatie
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20011 | 2500 AE | Den Haag

e-mail: 5.1.2.e @minbzk.nl
telefoon secretariaat: 5.1.2.e | mobiel: 5.1.2.e

3

5.1.2.e

Van: 5.1.2.e
Verzonden: zaterdag 1 oktober 2022 16:38
Aan: 5.1.2.e 5.1.2.e@tweedekamer.nl'; 5.1.2.e
Onderwerp: Woordvoeringslijn, eerste versie

Collega's,

Zoals beloofd even de woordvoeringslijn zoals die nu is op de mail:

- We zijn op de hoogte gebracht door ID-ware van een cyberaanval op hun systemen. ID-Ware levert diensten aan de Rijksoverheid, Eerste Kamer en Tweede kamer.
- ID-Ware heeft geconstateerd dat er bestanden naar buiten zijn gebracht door criminelen
- Er wordt door ID-Ware onderzoek gedaan of gegevens van klanten zijn gelekt. Zij worden daarbij ondersteund door een cybersecurity bedrijf.
- Rijksoverheid, Eerste kamer en Tweede Kamer houden de situatie goed in de gaten en hebben het NCSC gevraagd in dit incident te ondersteunen.
- We wachten de resultaten van het onderzoek af en zullen betrokkenen informeren als blijkt dat hun gegevens in de gelekte bestanden voorkomen.
- Er is wel al een voorlopige melding aan Autoriteit Persoonsgegevens gedaan.

Groet,

5.1.2.e

5.1.2.e

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Directie CIO Rijk | DG Overheidsorganisatie
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20011 | 2500 AE | Den Haag

e-mail: 5.1.2.e @minbzk.nl
telefoon secretariaat: 5.1.2.e | mobiel: 5.1.2.e

Concept communicatie n.a.v. ID-ware incident

Versie: 2 oktober 2022

In het incident overleg zijn 3 scenario's benoemd waarop communicatie nodig is rond de hack op ID-ware en de impact hiervan op de overheid. Dit document beschrijft de scenario's en de handelingswijze. Het is bedoeld om met woordvoering en de verschillende betrokken organisaties te verbeteren en een gemeenschappelijke communicatie te hanteren.

Scenario 1:

ID-ware heeft onderzoek gedaan en heeft bevestigd dat er gegevens van EK, TK en/of Rijksoverheid is gelekt. Het is niet publiek gemaakt.

Afweging:

Betrokkenen van wie de gegevens zijn gelekt moeten geïnformeerd worden. Niet van iedereen is een e-mail adres bekend en ook is dit een formele berichtgeving. Daarom

- Brief naar betrokkenen om hen te informeren.
- StassBZK informeren vanwege portefeuille Rijksdienst.
- Brief aan TK opstellen

Concept communicatie aan betrokkenen:

5.1.2.i/5.2.1

[redacted]

Scenario 2:

In de media wordt melding gedaan over de hack bij ID-ware en de impact op de overheid.

Afweging: dit bericht kan onrust veroorzaken bij medewerkers. Er is nog geen bevestiging van ID-ware, maar bronnen in de media kunnen betrouwbaar zijn. Er is niet bekend welke personen in het datalek zijn. Daarom:

- Bericht op Rijksportaal/Intranet

Concept tekst:

5.1.2.i/5.2.1

[redacted]

5.1.2 i/5.2.1 [redacted]

Scenario 3:

Er komen persvragen bij woordvoering binnen over de hack bij ID-ware

Afweging: pers krijgt de actuele woordvoeringslijn. Omdat waarschijnlijk snel scenario 2 zal starten, ook de actie bij scenario 2 uitvoeren.

Actuele woordvoeringslijn:

- We zijn op de hoogte gebracht door ID-ware van een cyberaanval op hun systemen. ID-Ware levert diensten aan de Rijksoverheid, Eerste Kamer en Tweede kamer.
- ID-Ware heeft geconstateerd dat er bestanden naar buiten zijn gebracht door criminelen
- Er wordt door ID-Ware onderzoek gedaan of gegevens van klanten zijn gelekt. Zij worden daarbij ondersteund door een cybersecurity bedrijf.
- Rijksoverheid, Eerste kamer en Tweede Kamer houden de situatie goed in de gaten en hebben het NCSC gevraagd in dit incident te ondersteunen.
- We wachten de resultaten van het onderzoek af en zullen betrokkenen informeren als blijkt dat hun gegevens in de gelekte bestanden voorkomen.
- Er is wel al een voorlopige melding aan Autoriteit Persoonsgegevens gedaan.

5

5.1.2.e

Van: 5.1.2.e
Verzonden: zondag 2 oktober 2022 13:34
Aan: cert@ncsc.nl
Onderwerp: FW: Aanvullende vragen m.b.t. hack ID-Ware

Ten behoeve van het onderzoek ID-ware, voor 5.1.2.e en 5.1.2.e. Is besproken.

Groet,
5.1.2.e

5.1.2.e

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Directie CIO Rijk | DG Digitalisering en Overheidsorganisatie
Turfmarkt 147 | 2511 DP | Den Haag
e-mail: 5.1.2.e @minbzk.nl
mobiel: 5.1.2.e | telefoon secretariaat: 5.1.2.e

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Datum: zondag 02 okt. 2022 10:45 AM
Aan: 5.1.2.e <5.1.2.e @minbzk.nl>
Kopie: 5.1.2.e @eerstekamer.nl <5.1.2.e @eerstekamer.nl>, 5.1.2.e <5.1.2.e @minbzk.nl>, 5.1.2.e <5.1.2.e @tweedekamer.nl>, 5.1.2.e @eerstekamer.nl <5.1.2.e @eerstekamer.nl>
Onderwerp: Aanvullende vragen m.b.t. hack ID-Ware

Goedemorgen 5.1.2.e,

Wij hebben vanuit de Tweede Kamer verschillende aanvullende vragen richting Rijks-CISO, NCSC of ID-Ware. Omdat we gister hebben besproken dat de regie bij Rijks-CISO ligt, leggen we deze vragen graag aan jou voor:

1) Op 19 september ontdekt ID Ware het incident. Dit omdat bepaalde systemen niet meer online zijn. Waarom heeft ID Ware dit niet eerder gezien via de monitoring op hun systemen? Of had ID Ware geen monitoring ingericht?
2) Welke maatregelen zijn exact ingericht na ontdekking van het incident? En welke beveiligingsmaatregelen had ID Ware voor die tijd ingericht om kwaadaardige infiltratie te voorkomen?
3) Gesteld is dat ID Ware ISO 27001 gecertificeerd is. Hebben wij dat certificaat? Dit om na te gaan waarop de certificering betrekking heeft en of er delen van ISO hiervan zijn uitgezonderd.
4) Is de data in de database OCMS versleuteld opgeslagen. Zo ja, met welke versleuteling? Kan de hacker toegang hebben gekregen tot de applicatie om de data onversleuteld te lezen, op te slaan, te exfiltreren?
5) Is er een backup van de OCMS dbase? Zo ja, waar staat die. Is dat een offline backup? Is de data daarop versleuteld?
6) Maakte ID Ware kopieën van de data in de OCMS dbase? Bijvoorbeeld dumps in andere formats? Zo ja, waarom gebeurde dat en waar waren die opgeslagen? En was dat versleuteld of onversleuteld?
7) Op welke wijze wordt de data richting de drukker van de rijkspassen verstuurd? Gebeurt dat via een beveiligde verbinding? Is die verbinding ook geraakt bij de hack?
8) Is aangifte gedaan van de hack? Ook in Duitsland? Zijn er ook Duitse onderzoeksinstanties aangehaakt bij het onderzoek?
9) Per wanneer is het onderzoek naar verwachting afgerond? Wanneer krijgt de TK als klant de rapportages hierover?

10) Op welke manier wordt zekergesteld dat bij ID Ware sprake is van een schone situatie? In die zin dat hun systeem vrij is van infiltratie?
11) Welke data van de Tweede Kamer is bij ID Ware voorhanden, naast de pasgegevens? Is deze andere data onderdeel van de hack? Zit dat tussen de 40 tot 70.000 gelekte bestanden?
12) Is het Rijk al afgekoppeld ja/nee zijn daar bepaalde overwegingen / risico's bij?
13) Heeft Ciso Rijk al NBV ingeschakeld / wordt er onderzocht of actoren in systemen zijn gekomen / konden komen?
14) Is bij ID ware bekend wie de hacker is? Stast men daarmee in contact? Is losgeld gevraagd? Is losgeld betaald en zo ja hoeveel?

We spreken elkaar vandaag om 12:00uur, dan kunnen we dit nader toelichten.

Groet,
Mede namens 5.1.2.e ,

5.1.2.e

Met vriendelijke groet,

5.1.2.e

Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA Den Haag
T 5.1.2.e
E 5.1.2.e@tweedekamer.nl | www.tweedekamer.nl

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Verslag integraal overleg 03-10-2022

Aanwezigen:

NCTV - afdeling Cybersecurity, vertegenwoordiger Cyber info intel Cell (CiiC), Team High Tech Crime (THTC), CISO Rijk, BZK, CISO TK, BVA Rijk & EK, CISO EK en NCSC.

Beeldvorming:

De CEO van ID Ware belt samen met een medewerker in. Zij geven het volgende aan:

- Ransomware is in de nacht van 16-09 op 17-09 uitgerold bij ID Ware, zondag ontdekt.
  Niet betaald, gedeeld gelocked.
- [redacted] vanaf 19-09 aangehaakt
- Actor BlackCat ALPHV.
- 4 minuten na middernacht is een admin account gevonden dat software had gestolen. Politie heeft de documentatie.
- 29-30 september is data gepubliceerd op het darknet
- 1 oktober om 10.30 uur telefoontje ID Ware 5.1.2f naar THTC-piket
- ID Ware heeft ook klanten in België en VK
- Mogelijk rond de 40.000 - 45.000 gegevens (Nederlands en Duits) ontvreemd. Nu onderzoek of er ID- / (vertrouwelijke) persoongegevens zijn gestolen.
- Wordt onderzocht welke data er is gestolen
- VPN verbinding was niet binnen scope forensisch onderzoek, eerst prioriteit op back-up en restore services. (5.1.2f [redacted]).
- Verwachting is dat er volgende week na het reviewen bevindingen van [redacted] gedeeld kunnen worden.
- Mogelijk tot 221 Gigabyte aan data ontvreemd
- ID Ware wil zsm meeting organiseren met projectmanager van [redacted] om de lijst te te laten delen.
- Situatie in Duitsland: logs met data, maar geen process- of customerdata en geen keys gevonden tot nu toe.
- Situatie in NL: operational Manager NL geeft aan dat slachtoffers per brief vanuit CEO (engelstalig) geinformeerd zijn in de gevallen waarvan huisadressen zijn gevonden. NCSC wil lijst met alle slachtoffers in NL hebben voor landelijk beeld. IB Ware gaat als eerste SAAS-customers met NCSC delen.
- Contactpersoon ID Ware die slachtoffercommunicatie doet koppelen aan NCSC-Iron piket

THTC:

- Onderschrijft delen van het verhaal van ID Ware.
- Geeft aan sinds 01-10 in contact te staan met ID Ware en 5.1.2f
- Bevonden dat een deel van de data bestond uit maintenance scripts en contact over sales.
- Hebben 1 IP-adres ontvangen van 5.1.2f. Dit lijkt echter een oud spoor.
- Op dit moment zijn zij nog niet overtuigd dat er informatie uit gevoelige databases is ontvreemd.
- Geven aan ID Ware morgen aangifte gaat doen. Zij verwachten dan meer informatie te ontvangen.

CISO Rijk:

- Geven aan dat eigenaarsschap van Rijks- en Kamerpassen bij (onderdelen van) CIO Rijk ligt.
- Onderschrijft het beeld van de politie dat fileservers geraakt zijn en niet databaseservers met gevoelige / vertrouwelijke gegevens.
- Geef aan dat er mogelijk van 3.500 medewerkers van de Belastingdienst naam, pasnummer en handtekening geexfiltreerd zou zijn. Waarschijnlijk staat hier geen thuisadres bij.
- BZK wijst er op dat er mogelijk tot 221 Gigabyte gestolen is en dat het onderzoek nog lang kan duren.
- Om 12.30 uur praat hij de Staatssecretaris BZK (en Woordvoering BZK) bij.

CISO Tweede Kamer:

- is op 21-09 op de hoogte gesteld. Eerste contact gericht op dienstverlening en niet op hack zelf.
- Interne crisisstructuur is op 30-09 geactiveerd. (OCT actief, ook bestuurlijke commissie CT)
- Geeft aan dat connecties met ID Ware zijn stilgezet. 5.1.2f [redacted]
- Verschillende typen pashouders, waarin kwaadwillende(n) interesse hebben.
  Op dit moment geeft TK geen Rijkspassen meer uit en voert geen wijzigingen door. Rijkspassen worden niet naar adressen gestuurd.
- Verbinding pas openstellen als dat weer veilig kan. 5.1.2n [redacted]
- Op dit moment zijn er geen indicaties dat de kwaadwillende(n) zijn doorgesprongen naar andere onderdelen van het netwerk.
  Monitoring wordt opgevoerd. [redacted] maakt onderdeel uit van Security Team TK. Mogen na overleg schakelen met collega's [redacted] van ID-Ware.
- Geeft aan dat de Tweede Kamervoorzitter is geinformeerd, De Eerste Kamervoorzitter en het presidium mogelijk (nog) niet.
- Daarnaast geeft hij aan dat gebruikers nog niet zijn geinformeerd
  - Het is nog onduidelijk wat voor / over wie informatie zou zijn ontvreemd
  - nog geen handelingsperspectief
- SBVA TK schakelde dit weekend met NCTV Bewaken en Beveiligen.
- Benadrukt dat Woordvoering belangrijk is.

BVA Rijk en Eerste Kamer:

- Initieel het signaal van Rijkspasbeheer gekregen dat de impact mee zou vallen.
- Geeft aan dat de VPN lijn FMH is vrijgegeven, maar dat zij daar niet gerust op zijn
- Toen bloeek dat er toch data gelekt was, direct CISO Rijk gebeld

CISO Eerste Kamer:

- Geeft aan dat een oud normenkader is ontvreemd. Een normenkader geeft technische details weer van passen.
  Onduidelijk welke versie is ontvreemd en wat de impact daarvan zou kunnen zijn. Oude versie staat ook op intranet via CIO Beraad.
- Vraagt zich af of een pas duplicaarbaar/reproduceerbaar is.

BZK:

- Geeft aan dat het onduidelijk is of een betrokken actor statelijk is.
- Onduidelijk of de aanval toeval of gericht is.
- Vraagt aandacht voor eerdere incidenten bij de Rijksoverheid. Onduidelijk wat een (mogelijk statelijke) actor al weet.
- Een mogelijk zachte link zou de initial access broker kunnen zijn.

NCSC

- Ransomware as a Service actor
- 5.1.2 f

<u>Oordeelsvorming</u>

Belangrijke punten zijn:

- Welke data zit in de 221 Gigabyte aan ontvreemde data? Duurt nog maand voor dat duidelijk is.
- Zorgen door Rijks BVA geuit over de VPN connectie Tweede Kamer (beheert het ook voor de Eerste Kamer)
  Tweede Kamer heeft VPN lijn afgesloten.
- Zorgen over integriteit Rijkspassen.
- Zorgen over sleutelmateriaal (VPN en mogelijk paslezers) waardoor toegang tot rijksgebouwen in geding is.
  CIO Rijk en BVA Rijk gaan daar achteraan.
- Communicatie:
  - Communicatie richting Kamerleden
  - Communicatie vanuit ID Ware is al gebeurd, gaat het rondzingen?
  - Woordvoeringslijn op orde hebben voor het geval het uitlekt
  - ID-Ware, TK en EK al gemeld bij AP

<u>Besluitvorming</u>

- NCSC gaat samen met Politie en diensten samenwerken
  NCSC zal als informatieknooppunt fungeren
- NCSC gaat samen met THTC een overleg inplannen met 5.1.2 f en ID Ware voor delen klantenlijst (of geprioriteerde delen klantenlijst)
  5.1.2 h
- Alle operationele contacten lopen via NCSC (5.1.2 e) en THTC (5.1.2 e)
- Tweede Kamer deelt technisch onderzoek met NCSC en NBV.
- Deelnemers sturen contactgegevens naar NCSC management piket.
- Communicatie: voorbereiden op bekendmaking hack / lekken van gegevens.

7

5.1.2.e

Van: 5.1.2.e <5.1.2.e @minbzk.nl>
Verzonden: donderdag 6 oktober 2022 21:02
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: Opzet brief ID-ware 0.1 rev aj.docx

5.1.2.e

Tot slot voor de volledigheid. Met betrekking tot de gemaakte afspraken verwijs ik je naar 5.1.2.e
En de impact van de hack schatten wij anders in dan jij en dat komt ook voort uit de berichten van TK en check hierop van NCSC.

Fijne avond verder.

Met vriendelijke groet,

5.1.2.e

T + 5.1.2.e
E 5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>

Van: 5.1.2.e <J5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>
Datum: donderdag 06 okt. 2022 8:55 PM
Aan: 5.1.2.e <5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>
Kopie: '5.1.2.e ' <5.1.2.e @tweedekamer.nl<mailto:5.1.2.e @tweedekamer.nl>>, '5.1.2.e '
<H5.1.2.e @tweedekamer.nl<mailto:H5.1.2.e @tweedekamer.nl>>, 5.1.2.e
<5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>, 5.1.2.e
<5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>, '5.1.2.e @eerstekamer.nl'
<5.1.2.e @eerstekamer.nl<mailto:5.1.2.e @eerstekamer.nl>>
Onderwerp: RE: Opzet brief ID-ware 0.1 rev aj.docx

Beste 5.1.2.e

Ik vind het dan toch bijzonder dat die afspraak mij niet bekend is. Bovendien kregen wij vragen van onze gebruikersorganisaties en juist om onrust en zorgen weg te nemen is er vanmiddag op mijn aangeven een kort communicatiebericht uitgegaan naar de contactpersonen van onze gebruikersorganisaties. Dat zag er als volgt uit:

Recent is bekend geworden dat een leverancier van Rijkspas is getroffen door een cyberaanval.
Dit betreft géén hack op de centrale Rijkspasinfrastructuur bij ODC-Noord en SSC-ICT, maar raakt uitsluitend de serveromgeving van de leverancier.
De Rijkspas infrastructuur 5.1.2.h is dus niet gecompromitteerd!

Wij hebben overigens van geen enkele organisatie een aanvullende reactie of vragen op ons bericht gekregen, anders dan dankjewel.

Als er daadwerkelijk bloed uit dit berichtje kan vloeien, dan mag je dat mij verwijten, maar ik wil je vriendelijk vragen om het niet groter te maken dan het is.
We doen allemaal ons best om dit tot een goed einde te brengen en gezien de onderzoeksbevindingen denk ik dat we alle reden hebben om juist de kalmte te bewaren en de politiek te informeren dat de hack natuurlijk heel vervelend is, maar dat de impact gering is en alle betrokken partijen netjes zijn/worden geïnformeerd.

Ik bel je morgen ook nog wel even.

Vriendelijke groet,

5.1.2.e

Van: 5.1.2.e <5.1.2.e @minbzk.nl>
Verzonden: donderdag 6 oktober 2022 19:40
Aan: 5.1.2.e <5.1.2.e @minbzk.nl>
CC: 5.1.2.e @tweedekamer.nl>; 5.1.2.e ' <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e @eerstekamer.nl' <5.1.2.e @eerstekamer.nl>
Onderwerp: RE: Opzet brief ID-ware 0.1 rev aj.docx

5.1.2.e

Het gaat mij om de deze week tussen alle betrokken organisaties gemaakte afspraak dat wij op hetzelfde moment als Rijksdienst, Eerste en Tweede Kamer, zouden gaan communiceren én op aangeven van 5.1.2.e (die wij de coördinatie hebben gegeven). Dit communiceren zou vlak voor het versturen van de Kamerbrief plaatsvinden met dan volgend de brief.

Door zelf als Rijkspasbeheer - afgezien van de inhoudelijke argumenten hiervoor - te gaan communiceren breng je de Tweede en Eerste Kamer is een lastige positie en zijn wij al uren bezig 'de geest in de fles' te krijgen. Want de kans is nu dat het extern bekend wordt zonder dat wij intern gecommuniceerd hebben en dat willen wij niet. Daarnaast doorkruis je hiermee het politieke traject van het zorgvuldig schriftelijk informeren van de Tweede Kamer. Ook daar is de kans nu aanwezig dat men het uit het 'nieuws' gaat vernemen.

Met vriendelijke groet,

5.1.2.e
5.1.2.e

T + 5.1.2.e
E 5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>

Van: 5.1.2.e <J5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>
Datum: donderdag 06 okt. 2022 5:52 PM
Aan: 5.1.2.e <5.1.2.e @minbzk.nl<mailto:m5.1.2.e @minbzk.nl>>
Kopie: 5.1.2.e 5.1.2.e @tweedekamer.nl<mailto:5.1.2.e @tweedekamer.nl>>, 5.1.2.e ' <5.1.2.e @tweedekamer.nl<mailto:5.1.2.e @tweedekamer.nl>>, 5.1.2.e <5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>, 5.1.2.e <J5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>, '5.1.2.e @eerstekamer.nl' <5.1.2.e @eerstekamer.nl<mailto:5.1.2.e @eerstekamer.nl>>
Onderwerp: RE: Opzet brief ID-ware 0.1 rev aj.docx

Beste 5.1.2.e

Ik wil graag even reageren op jouw reactie dat je niet blij ment met onze communicatieactiviteiten en je opmerking dat er mogelijk wel iets aan de hand is wat niet uit de brief van ID-ware zou blijken.

1. Er is ook hier een onderscheid tussen ID-ware als leverancier van 5.1.2.f aan de Tweede Kamer en communicatie vanuit CIO Rijk als eigenaar van de rijksbrede Rijkspas voorziening. In het eerste geval heeft ID-ware zich te houden aan de afspraken. Ik heb dit nagevraagd en ID-ware heeft mij bevestigd dat zij zich netjes aan deze afspraak heeft gehouden en dus niet zelfstandig heeft gecommuniceerd. In het tweede geval ben ik namens 5.1.2.e en is het mijn verantwoordelijkheid om gebruikersorganisaties te informeren (en gerust te stellen) over een hack bij een van onze leveranciers. Dat hebben we op twee manieren gedaan; Een bericht naar onze Rijkspas klantgroep (verstuurd door 5.1.2.e en een bericht vanuit de Rijkspas servicedesk (ook bekend onder naam Rijkspasbeheer) naar onze DAP contactpersonen met uitsluitend de melding dat er een hack heeft plaatsgevonden, maar dat de Rijkspas infrastructuur niet is geraakt (essentieel gegeven!). Daarbij zijn geen namen van organisaties genoemd.
2. Ik heb ID-ware gevraagd contact op te nemen met NCSC. Reactie van het NCSC was dat zij naar de TK hebben bevestigd dat er een leak lijst is. NCSC en de politie hebben die lijst ook ontvangen. Op de lijst staan geen bestanden op de van de Eerste en Tweede Kamer. De leaklijst bevat uitsluitend bestanden van andere klanten van ID-ware. Kun je misschien aangeven wat je bedoelt met 'dat er iets aan de hand'? Dan kunnen we dat ook gericht nagaan.

Vriendelijke groet,

5.1.2.e

Van: 5.1.2.e <5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>
Verzonden: donderdag 6 oktober 2022 15:01
Aan: 5.1.2.e ' <5.1.2.e @tweedekamer.nl<mailto:5.1.2.e @tweedekamer.nl>>; 5.1.2.e <5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>; 5.1.2.e <5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>; 5.1.2.e <5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>; 5.1.2.e @eerstekamer.nl' <5.1.2.e @eerstekamer.nl<mailto:5.1.2.e @eerstekamer.nl>>
CC: 5.1.2.e <5.1.2.e @tweedekamer.nl<mailto:5.1.2.e @tweedekamer.nl>>
Onderwerp: RE: Opzet brief ID-ware 0.1 rev aj.docx

5.1.2.e

Eens met commentaar 5.1.2.e , daarnaast ben ik buitengewoon ongelukkig met het feit dat vanuit Rijkspasbeheer zelfstandig gecommuniceerd is zonder overleg met Eerste en Tweede Kamer. Dit was niet de afspraak.

Wij gaan nu vanuit de Eerste en Tweede Kamer vandaag zelfstandig communiceren want bij ons is wel wat aan de hand (bevestigd door NCSC) en volgens Rijkspasbeheer bij hun niet. Daarnaast heeft ANP eerste vraag al aan Tweede Kamer gesteld.

Met vriendelijke groet,

5.1.2.e

5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl<mailto:5.1.2.e @tweedekamer.nl>>
Verzonden: donderdag 6 oktober 2022 14:26

Aan: 5.1.2.e <5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>; 5.1.2.e
<5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>; 5.1.2.e
<5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>; 5.1.2.e
<5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>
CC: 5.1.2.e <5.1.2.e @tweedekamer.nl<mailto:5.1.2.e @tweedekamer.nl>>
Onderwerp: RE: Opzet brief ID-ware 0.1 rev aj.docx

Hierbij alvast mijn commentaar. 5.1.2.e staat in de cc.

Met vriendelijke groet,

5.1.2.e
Tweede Kamer der Staten-Generaal Postbus 20018, 2500 EA
5.1.2.e
T +5.1.2.e | 5.1.2.e @tweedekamer.nl<mailto:5.1.2.e > | I
www.tweedekamer.nl<http://www.tweedekamer.nl/>

Van: 5.1.2.e 5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>
Verzonden: donderdag 6 oktober 2022 14:04
Aan: 5.1.2.e <5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>; 5.1.2.e
<5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>; 5.1.2.e
<5.1.2.e @tweedekamer.nl<mailto:5.1.2.e @tweedekamer.nl>>; 5.1.2.e
<5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>
Onderwerp: Opzet brief ID-ware 0.1 rev aj.docx

Beste 5.1.2.e 5.1.2.e 5.1.2.e

Bijgaand de eerste aanzet voor een kamerbrief, die voor het weekend naar de kamer gaat. Graag jullie kritische blik en aanvullingen/opmerkingen.

Groet

5.1.2.e

Duiding mediaberichtgeving

Berichtgeving nav Kamerbrief op 7 oktober
Het verzenden van de Kamerbrief op vrijdag heeft tot media-aandacht geleid. Op vrijdag 7 oktober is er op meerdere nieuwssites aandacht besteed aan de hack. Een overzicht daarvan zoals opgesteld door MinJenV is bijgevoegd (bijlage 4c), evenals de artikelen zelf. Men beperkt zich vooral tot feitelijke duiding met de Kamerbrief als brondocument. Er wordt in enkelen gevallen foutief gesteld dat er gegevens van Kamerleden gelekt zijn.

ID-ware statement
Statement ID-ware 7 oktober
Naar aanleiding van de deels onjuist berichtgeving, heeft ID-ware op 7 oktober een incident statement uitgebracht (zie bijlage 4d). Dit statement is niet afgestemd met de overheid. In het statement beschrijft men kort wanneer men achter het incident kwam, en wat men sindsdien gedaan heeft. Ook betuigt men spijt over het incident, en wordt de samenwerking met de overheid benoemd. Het statement meldt in reactie op de berichtgeving twee belangrijke punten:

1) Het statement stelt dat "ID-ware kan bevestigen dat uit onderzoek tot op heden niet is gebleken dat er data van Kamerleden of andere publieke personen bij het datalek betrokken zijn." Dit statement komt voor rekening van ID-Ware, en kunt u niet bevestigen of ontkennen. Wat u heeft aangegeven aan de Kamer is dat er ongeveer 3500 namen zijn gelekt. Dat aantal is bevestigd in ID-Ware in contact met de overheid, en ook door 5.1.2.f, die het onderzoek doen. Ambtenaren, wiens gegevens gelekt zijn, zijn werkzaam in het publieke domein.

2) Het statement stelt verder dat de aanval zou zijn uitgevoerd door de bekende ransomware groep BlackCat, ook bekend als AHLPV. In verband met het nog lopende onderzoek van onder andere de politie, kunt u deze stelling niet bevestigen of ontkennen.

Dit statement was ook aanleiding voor media-berichtgeving, maar minder dat de kamerbrief op 7 oktober. Over het statement van ID-Ware hebben de Volkskrant, het Nederlands Dagblad, RTL nieuws, security.nl en PZC gepubliceerd.

IDware

Incident Statement – ID-ware

Op zondag 18 september heeft ID-ware vastgesteld dat een deel van haar IT-servers niet meer beschikbaar was. ID-ware bleek slachtoffer te zijn van een ransomware aanval. ID-ware heeft daarop direct actie ondernomen en gehandeld in lijn met de geldende wet- en regelgeving: binnen 24 uur zijn gerenommeerde externe cyber security experts aan de slag gegaan, die een onderzoek hebben uitgevoerd naar de aard van de aanval en de betrokken gegevens. De operatie kon snel hersteld worden en de veiligheid van de systemen is verder aangescherpt. Helaas bleek uit verder onderzoek dat de data van een aantal klanten van ID-ware is getroffen door de aanval.

ID-ware betreurt dit zeer en doet er alles aan om ervoor te zorgen dat de gevolgen voor de getroffen klanten zo klein mogelijk zijn. ID-ware heeft een verzoek tot losgeld gekregen waar zij geen gehoor aan heeft gegeven. Er is melding gedaan bij de Autoriteit Persoonsgegevens, ID-ware is in voortdurend contact met de politie, overheid en het Nationaal Cyber Security Centrum.

De ransomware-aanval is uitgevoerd door de bekende ransomware-groep "BlackCat" alias "AHLPV". De gelekte data is gepubliceerd op het darkweb. De externe cyber security experts hebben ID-ware een lijst aangereikt met daarin de bestandsnamen van de gepubliceerde data. Klanten van onze diensten waarvan is vastgesteld dat er gegevens zijn gelekt, zijn direct geïnformeerd.

ID-ware kan vanwege vertrouwelijkheid geen mededelingen doen over haar individuele klanten. Wel kan ID-ware bevestigen dat uit het onderzoek tot op heden niet is gebleken dat er data van Kamerleden of andere publieke personen bij het datalek betrokken zijn. Ook verschaft de bij het datalek betrokken informatie op geen enkele manier toegang tot rijksgebouwen: ID-ware beschikt niet over het hiervoor benodigde sleutelmateriaal.

Maatregelen

Op advies en met ondersteuning van haar externe cyber security experts heeft ID-ware direct een aantal aanvullende veiligheidsmaatregelen getroffen, om enig potentieel restrisico te limiteren en om de bron van het incident te identificeren om zo herhaling in de toekomst te voorkomen. Dit omvat o.a. een veiligheidsscan van de herstelde servers, laptops en PCs, een reset van wachtwoorden, extra controle op administrator accounts en aanvullende 24-uurs externe SOC (Security Operation Center) - monitoring ingeschakeld om direct verdachte activiteit te kunnen identificeren.

ID-ware neemt deze situatie zeer serieus en begrijpt de zorgen van klanten en gebruikers van onze diensten. Wij willen benadrukken dat deze situatie voor ons de grootste prioriteit heeft. Externe professionals zijn ingeschakeld en voortdurend betrokken. Op dit moment is ID-ware bezig de totale omvang van de aanval vast te stellen. We monitoren de gevolgen en houden onze klanten van de voortgang op de hoogte.

Over ID-ware

ID-ware ontwikkelt software en levert diensten voor toegangsoplossingen die in verschillende sectoren gebruikt worden. ID-ware is met name actief in de Europese markt. ID-ware heeft ongeveer 100 werknemers en een track-record van bijna 20 jaar in deze markt en is sinds lange tijd ISO 27001 en 9001 gecertificeerd.

10

5.1.2.e

Van: 5.1.2.e
Verzonden: vrijdag 7 oktober 2022 15:51
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: Hack ID-ware

Beste allemaal,

Zal jullie niet ontgaan zijn dat ID-ware, softwareleverancier van onze card management software, is gehackt. In de pers verschijnen meerdere berichten die maar deels juist zijn.
De coördinatie van het onderzoek naar ID-ware vanuit het Rijk vindt plaats o.l.v. 5.1.2.e en is daarmee in prima handen.

De berichtgeving heeft mij aanleiding gegeven om nog wat extra vragen te stellen.
Met name ging het mij om eventuele verbindingen tussen ID-ware infra en Rijkspas-infra centraal, en met betrekking tot de verwerking van persoonsgegevens.

Ik heb het volgend teruggekregen op deze vragen (met dank aan 5.1.2.e):

- ➔ Er is geen fysieke koppeling tussen het netwerk van ID-ware en de Rijksoverheid
- ➔ Er staan geen persoonsgegevens van medewerkers van BZK op systemen bij ID-ware. Buitgemaakte persoonsgegevens zouden derhalve geen betrekking kunnen hebben op gegevens van medewerkers van BZK.

De definitieve resultaten van het onderzoek moeten nog komen, ik ga ervan uit dat dit geen nieuwe inzichten t.o.v. bovenstaande gaat geven.

Voor een link naar de brief van de Staatssecretaris aan de Tweede Kamer:
https://www.tweedekamer.nl/downloads/document?id=2022D40458

Vriendelijke groet, 5.1.2.e

p.s.: de Eerste Kamer en Tweede Kamer hebben eigen afspraken met ID-ware, vandaar dat je deze organisaties ook tegenkomt in de berichtgeving.

11

5.1.2.e

Van: Rijksoverheid <rijksoverheid-bounces@lists.ncsc.nl> namens Info (NCSC-NL) <info@ncsc.nl>
Verzonden: vrijdag 7 oktober 2022 15:00
Aan: Info (NCSC-NL)
Onderwerp: [Rijksoverheid] [TLP:AMBER] Berichtgeving rondom de hack bij ID-ware

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

[TLP:AMBER]

Beste NCSC-partner,

U ontvangt dit doelgroepbericht in verband met een ransomware-aanval op het bedrijf ID-ware. ID-ware heeft verschillende klanten, waaronder de Rijksoverheid. De staatssecretaris Digitalisering heeft de Tweede Kamer vandaag geïnformeerd over deze casus (1).

Mogelijk bent u, of is een toeleverancier van u, klant van ID-ware. In dat geval heeft de ransomware-aanval mogelijk impact op uw organisatie. Het doel van dit bericht is u te informeren over de ransomware-aanval en handelingsperspectief te bieden.

Feiten:

· Op 27 september 2022 zijn er gegevens van het bedrijf ID-ware aangeboden op de blog van de criminele actor ALPHV/BlackCat. ALPHV/BlackCat is een criminele organisatie die ransomware-as-a-service aanbiedt. Er zijn sinds eind 2021 tientallen organisaties slachtoffer geworden van ALPHV/BlackCat ransomware. (2) · ID-ware is een leverancier van fysieke beveiligingsoplossingen voor verschillende organisaties, waaronder ook organisaties in Nederland.
ID-ware biedt voornamelijk oplossingen voor toegangsbeheer d.m.v.
gepersonaliseerde kaarten (smart cards). (3) · Aanvallers hebben onlangs toegang verkregen tot sommige systemen van ID-ware en hebben daar een ransomware-aanval op uitgevoerd.
· De beschikbaarheid van de getroffen systemen van ID-ware kon na de ransomware-aanval snel worden hersteld. Wel hebben de aanvallers oneigenlijk toegang gekregen tot data die was opgeslagen op de systemen van ID-ware. Dit blijkt onder andere uit beperkte gepubliceerde gegevens op de leak site van ALPHV/BlackCat. (4) De aanvallers publiceren deze beperkte gegevens om de authenticiteit van de verkregen data te bevestigen. Uit de tot nu toe gepubliceerde gegevens kan het NCSC nog geen conclusie trekken over de omvang en implicaties van dit datalek.
· Het NCSC heeft de afgelopen dagen in nauw contact gestaan met ID-ware en verschillende partnerorganisaties om meer zicht te krijgen op de uitgevoerde digitale aanval en de (mogelijke) gevolgen ervan.

Duiding:

· Als u klant bent van ID-ware is het mogelijk dat gegevens die u met ID-ware heeft gedeeld zijn gelekt.
· ID-ware heeft aangegeven dat zij in contact staan met mogelijk getroffen klanten.
· ID-ware geeft ook aan dat met de gelekte informatie geen rijkspas kan worden gefabriceerd die toegang tot gebouwen geeft. Het hiervoor benodigde sleutelmateriaal wordt niet verwerkt bij ID-ware. Op dit moment heeft het NCSC geen indicaties dat sleutelmateriaal van eventuele andere (toegangs)passen geleverd door ID-ware in gevaar zijn geweest. Dit is nog onderwerp van verder onderzoek.

Handelingsperspectief:

· Als u klant bent van ID-ware is het belangrijk dat u in kaart brengt welke gegevens u heeft gedeeld met ID-ware. Houd er rekening mee dat deze gegevens mogelijk gelekt zijn.

· Indien u gebruik maakt van een toeleverancier die klant is van ID-ware, neem dan contact met hen op of er eventueel (persoons)gegevens van uw organisatie gelekt zijn.
· Bent u klant en heeft u (persoons)gegevens gedeeld, wees dan extra alert op mogelijke phishing, oplichting en identiteitsfraude.
· Wees voorbereid op eventuele vragen vanuit de media en uw stakeholders.

** ENGLISH VERSION **

Dear NCSC partner,

You are receiving this message following a ransomware-attack on ID-ware.
ID-ware has a variety of customers, including the Dutch government. The Minister for Digitilisation has informed the Dutch Parliament about this case. (1).

If you or your supplier are a customer of ID-ware, the ransomware-attack could impact your organisation. The aim of this message is to inform you about the attack and provide you with a recommended course of action.

Facts:

· On 27 September 2022 data from ID-ware was leaked on the blog of criminal actor ALPHV/BlackCat.
ALPHV/BlackCat is a criminal organisation that offers ransomware-as-a-service. Dozens of organisations have become victim of ALPHV/BlackCat ransomware since 2021. (2) · ID-ware provides physical security solutions for different organisations, including organisations in the Netherlands. ID-ware primarily provides solutions with regard to access management via personalised (smart) cards. (3) · Attackers have recently gained access to some of ID-ware's systems, which was followed by a ransomware attack.
· ID-Ware was able to quickly restore the availability of its compromised systems following the ransomware attack. However, the attackers were able to illegally obtain data stored on ID-ware's systems. Limited information was published on the leak site of ALPHV/BlackCat. (4) The attackers are publishing this limited set to prove the authenticity of the obtained data.
NCSC-NL cannot as of yet draw firm conclusions about the extent and impact of the leak based on the data published.
NCSC-NL has been in close contact with ID-ware and a number of partner organisations to get more insight into the digital attack and the possible consequences hereof.

Interpretation:

· If you are a customer of ID-ware, then it is possible that the data you have shared with ID-ware may have been leaked.
· ID-ware has stated that they are in close contact with customers that have (potentially) been affected by the leak.
· ID-ware also states that the leaked information cannot be used to fabricate a Rijkspas (a smart card that provides access to government buildings). The required key material is not processed by ID-ware. At this moment NCSC has no indication that key material of other smart cards produced by ID-ware have been compromised. This is subject of further investigation.

Advise:

· If you are an ID-ware customer, it is important that you investigate which data you have shared with ID-ware. Please note that this data may have been leaked.
· If you use a supplier that is an ID-ware customer, please contact them to verify if any (personal) data of your organization has been compromised.
· If you are an ID-ware customer and have shared (personal) data, be aware of potential phishing, fraud and identity fraud.
· Be prepared for any questions from the media and your stakeholders.

[TLP:AMBER]

Met vriendelijke groet / kind regards,

Nationaal Cyber Security Centrum
Postbus 117 | 2501 CC | Den Haag | www.ncsc.nl
E info@ncsc.nl
T +31 070 751 55 55 (algemeen)
PGP 486E F5E3 82B5 5BCA 1C66 A923 1CA9 5AAC 3F66 2B80
Bezoekadres:
Turfmarkt 147 | 2511 DP | Den Haag

(1)
https://www.tweedekamer.nl/kamerstukken/brieven_regering
/detail?id=2022Z18936&did=2022D40458

(2) https://www.ic3.gov/Media/News/2022/220420.pdf

(3) https://www.id-ware.com/nl/home.html

(4) https://twitter.com/Cyberknow20/status/1575113726222430208

-----BEGIN PGP SIGNATURE-----
Version: Encryption Desktop 10.4.2 (Build 1298) - not licensed for commercial use: www.pgp.com
Charset: utf-8

wsDVAwUBY0AiThypWqw/ZiuAAQr5jAwAxijnVvuJRp+GwAcssCIY2XDKgUUAMw83
EXi2KGY4LiLorPRxEZ6vNiUAyuAdOCma8A9OPb2FOT4KTNZC1e9DmdVYqUNY1Xmu
6hoGKMAe++SttiPe695iY2/CRMcdIhzNaG9IFWYS+LupxfROE5UzoOOQZNxNmoga
LtrICEmLC1brwJAwUvU5GSiaEdxmyUsKmFgf0vylJKBHtxJjDA55ya+FdHlfy0Z3
FEzm23Mt5f753j/b/4UPyllZqkjsHZW/aM02V/EZO/58A+KNu6rU0fGOqIwZqNAL
YHsiCI38Z2QZnP6Wi71MhbzKFfIHSwzw5OxxUawyy9+t6zFMNFZ8xQMoi+9oO5sS
cnMAhNqFQwL9KoSQNi18YvxrI6zKLU1w+gwYtnQQij3eHCt+LikNunDluxac4hU6
4Tbra0h88dZBa3RkCy1xGFKWMo9BIKrH57fwGsG+E64nsBFIY/hJIGPoKfvAAdFp
2+P0WIRZr4idm/gCg77Ha4PyV0vCmSS1
=IsaP
-----END PGP SIGNATURE-----

12

5.1.2.e

Van: 5.1.2.e
Verzonden: vrijdag 7 oktober 2022 14:20
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: Rijkspas

Dank 5.1.2.e,

M.b.t. het tweede was ik in verwarring omdat er volgens de nota van de stas gegevens van medewerkers van de rijksoverheid zijn geraakt (dat was ivm die thuisbezorgservice), maar dat niet kan uitgesloten worden dat nog andere gegevens van rijkspasgebruikers zijn gelekt.
Dat laatste zou dan, volgens jou niet betrekking kunnen hebben op rijksmedewerkers. IDWare heeft dus geen kopieën van onze persoonsgegevens op hun systemen, anders dan degene die blijkbaar (?) tijdelijk nodig waren ivm die thuisbezorgservice.

Groet, 5.1.2.e

Van: 5.1.2.e <5.1.2.e @minbzk.nl>
Verzonden: vrijdag 7 oktober 2022 14:12
Aan: 5.1.2.e <5.1.2.e @minbzk.nl>
CC: 5.1.2.e <5.1.2.e @minbzk.nl>
Onderwerp: RE: Rijkspas

Van: 5.1.2.e <5.1.2.e @minbzk.nl>
Verzonden: vrijdag 7 oktober 2022 14:07
Aan: 5.1.2.e <5.1.2.e @minbzk.nl>
CC: 5.1.2.e <5.1.2.e @minbzk.nl>
Onderwerp: Rijkspas

Hoi 5.1.2.e,

M.b.t. Rijkspas: ik weet dat 5.1.2.e daarmee bezig is, en dat is prima. Ik neem ook direct aan dat de impact op toegang duidelijk is, en in lijn met zoals eerder gecommuniceerd. We worden over het algemeen goed op de hoogte gehouden.

Ik heb echter een aantal vragen die geen onderzoek zouden hoeven te vergen, omdat dit direct bekend zou moeten zijn – het zou immers gebaseerd moeten zijn op staande afspraken met de leverancier. Die vragen komen wel voort uit onduidelijkheid in de berichtgeving tot nu toe.

1) Er wordt gesteld dat de centrale Rijkspasinfrastructuur niet is geraakt. Dat laat de mogelijkheid open dat dit wel had gekund, omdat ik in de formulering iets mis. Als het goed is, is de infrastructuur waar ID-ware zelf controle over heeft (dus hetgeen nu gehackt is) op geen enkele manier fysiek verbonden met de centrale Rijkspasinfrastructuur. Kun jij dat bevestigen?
   Dit klopt. Er is geen fysieke koppeling tussen het ID-ware netwerk en Rijksoverheid.

2) Al een paar jaar geleden hebben wij het gehad over productiegegevens in de test- en acceptatieomgevingen. We hebben toen afgesproken dat in test- en acceptatie geen productiegegevens mogen staan. Ik ben in de veronderstelling dat op spullen van IDWare geen, maar dan ook geen enkele persoonsgegevens van BZK-medewerkers staan. Klopt dat?
   Klopt, alle applicaties die gebruik maken van persoonsgegevens van Rijksmedewerkers staan enkel binnen de Rijksinfrastructuur en niet binnen de ID-ware omgeving.

Alvast dank voor je antwoord.

Groet, 5.1.2.e

13

5.1.2.e

Van: 5.1.2.e <5.1.2.e @minjenv.nl>
Verzonden: vrijdag 7 oktober 2022 12:51
Aan: 5.1.2.e
Onderwerp: RE: Communicatie

Dank!

Intern bewaken en beveiligen NCTV is op de hoogte.
Via de collega's heb ik nu uitgezet dat de DKDB ook collegiaal wordt geïnformeerd.

Dank voor attenderen,

Groet 5.1.2.e

Met vriendelijke groet,

5.1.2.e

.....
Ministerie van Justitie en Veiligheid
Nationaal Coördinator Terrorismebestrijding en Veiligheid
Nationale Crisisbeheersing en Bewaken en Beveiligen
Turfmarkt 147 | 2511 DP | Den Haag
Postbus20301 | 2500 EH | Den Haag
.....
M 5.1.2.e
5.1.2.e @nctv.minjenv.nl
secretaresse: 5.1.2.e @nctv.minjenv.nl
www.nctv.nl
.....

Van: 5.1.2.e <5.1.2.e @minbzk.nl>
Verzonden: vrijdag 7 oktober 2022 12:37
Aan: 5.1.2.e <5.1.2.e @minjenv.nl>; 5.1.2.e <5.1.2.e @minjenv.nl>
Onderwerp: Communicatie

Ha 5.1.2.e ,

Hebben jullie ook met DBB gecommuniceerd dat er berichtgeving komt?

Groet,

5.1.2.e

5.1.2.e

.....
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Directie CIO Rijk | DG Overheidsorganisatie
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20011 | 2500 AE | Den Haag
.....
e-mail: 5.1.2.e @minbzk.nl
telefoon secretariaat: 5.1.2.e | mobiel: 5.1.2.e

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

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Ministry of Justice and Security

14

5.1.2.e

Van: 5.1.2.e
Verzonden: vrijdag 7 oktober 2022 17:46
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: Q&A Hack

Hoi 5.1.2.e,

Ik ben ermee aan de slag maar ik wil wel alvast op de eerste twee reageren omdat die van essentieel belang zijn om juist te beantwoorden. Dat is nu niet het geval:

Q&A

Aanvulling Q&A volgt, maar ik vond het belangrijk om dit alvast met je te delen (het staat ook onjuist in het bericht op Rijksportaal).

Fijn weekend.

Vriendelijk groet,

5.1.2.e

Van: 5.1.2.e <5.1.2.e @minbzk.nl>
Verzonden: vrijdag 7 oktober 2022 16:46
Aan: 5.1.2.e <J5.1.2.e @minbzk.nl>
CC: 5.1.2.e <5.1.2.e @minbzk.nl>
Onderwerp: RE: Q&A Hack

Hoi 5.1.2.e

Dank voor het aanbod, heel handig als je kunt aanvullen. In de bijlage de Q&A die TK en EK gemaakt hebben, is volgens mij prima bruikbaar voor algemene woordvoering. Overigens beperk ik me in de woordvoering zoveel mogelijk tot de inhoud van de kamerbrief, maar handig om wat aanvullende info achter de hand te hebben.

Groet
5.1.2.e

Van: 5.1.2.e <5.1.2.e @minbzk.nl>
Verzonden: vrijdag 7 oktober 2022 16:14
Aan: 5.1.2.e <5.1.2.e @minbzk.nl>
CC: 5.1.2.e <5.1.2.e @minbzk.nl>
Onderwerp: Q&A Hack

Beste 5.1.2.e,

Van 5.1.2.e begreep ik dat jij de woordvoering rond de hack bij ID-ware op je hebt genomen.

Ik heb 5.1.2.e aangeboden om te helpen bij de Q&A (ook voor Kamervragen), vanuit mijn inhoudelijke kennis op dit dossier.

Is het een idee dat je de Q&A aan mij stuurt en ik kijk waar ik die kan aanvullen?

Met vriendelijke groet,

5.1.2.e

DGOO/CIO Rijk/ICT Voorzieningen en Infrastructuur Rijk
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Turfmarkt 147| 2511 DP | Den Haag
Postbus 20011 | 2500 EA | Den Haag

T 5.1.2.e
5.1.2.e @minbzk.nl

Aantekeningen overleg ransomware aanval op ID-ware

Versie: 9 oktober 21:00

Woensdag 21 september 2022

- 5.1.2.e neemt contact op met 5.1.2.e ivm een melding dat ID-ware te maken heeft met een digitale aanval. Dit kan impact hebben op gegevens van EK en TK die ivm het uitgeven van Rijkspassen bij ID-ware worden beheerd. Ook rijkspas Rijksoverheid word via ID-ware uitgegeven, maar Rijksoverheid beheart de gegevens zelf. Onderzoek loopt, verwacht wordt begin week 39 het resultaat te krijgen.

Vrijdag30 september 2022

- Nogmaals contact tussen 5.1.2.e en 5.1.2.e . ID-ware heeft een brief gestuurd met uitleg, maar kan nog niets zeggen over impact op gegevens van klanten. Wel is duidelijk dat er een grote hoeveelheid bestanden zijn gelekt via een bericht op darkweb. 5.1.2.f doet onderzoek, er gaat nog aangifte bij politie volgen. TK heeft inmiddels operationeel crisisteam ingericht. Zowel EK als TK hebben melding gedaan bij autoriteit persoonsgegevens.

- 5.1.2.e neemt contact op met NCSC. NCSC was wel al bekend met een mogelijke aanval op ID-ware, maar had nog geen melding gekregen. 5.1.2.e geeft aan dat deze melding mede namens TK is. In het overleg wordt de tot nog toe bekende informatie uitgewisseld en contactinformatie voor het weekend gedeeld.

Zaterdag 1 oktober 2022

- 11:30 Overleg tussen 5.1.2.e, 5.1.2.e en 5.1.2.e . Verzoek aan 5.1.2.e om regie te pakken namens de partijen, afspraak om gedurende het weekend samen het verloop in de gaten te houden. Inmiddels is duidelijk dat ook THTC van de Nationale Politie is aangehaakt, maar nog niet benaderd is. Afgesproken dat NCSC dit incident tussen de partijen gaat coordineren. Ook afgesproken dat we gezamenlijk optreden in communicatie: 5.1.2.e maakt een woordvoeringslijn voor het geval pers vragen stelt, er zal een gezamenlijk bericht gemaakt worden voor eventuele communicatie naar medewerkers. Het moment van communiceren hangt af van 1) het resultaat van onderzoek bij ID-ware als duidelijk wordt dat er gegevens zijn gelekt of 2) er in de media wordt gemeld dat er gegevens van EK, TK of Rijksoverheid zijn gelekt.

- 12:00 Overleg tussen 5.1.2.e en NCSC. Verzoek om ondersteuning wordt ook via mail gestuurd. Er is een team ingericht bij NCSC. Afgesproken dat NCSC contact zoekt met ID-ware, 5.1.2.f en THTC.
- 5.1.2.e informeert 5.1.2.e en 5.1.2.e via mail.
- 5.1.2.e informeert 5.1.2.e via mail en Signal. 5.1.2.e verzoekt 5.1.2.e stassBZK te informeren via mail

- 16:00 Overleg tussen 5.1.2.e, 5.1.2.e en 5.1.2.e . NCSC heeft nog geen contact kunnen krijgen met ID-ware. Wel met 5.1.2.f, deze geeft geen informatie en bevestigt ook niet dat ze zijn ingeschakeld door ID-ware. THTC is gesproken, zijn zeer geinteresseerd, maar hebben geen contact gehad met ID-ware. Er is nog geen informatie gevonden die naar een actor leidt. Wel is uit darkweb, via 5.1.2.e informatie gekomen, nu vooral over Duitse slachtoffers en namen van medewerkers van de Universiteit Utrecht. Op Social Media is verder nog geen ebrichtgeving, op één algemene tweet na die wijst op een volgend slachtoffer van groep ALPHV.

- 16:47 Contact tussen 5.1.2.e en 5.1.2.e (NCTV). Zij hebben wel contact gehad met ID-ware. ID-ware geeft aan graag te willen meewerken. Afgesproken dat DBB contact opneemt met NCSC om gegevens uit te wisselen.

- 20:00 Overleg tussen 5.1.2.e, 5.1.2.e, 5.1.2.e, 5.1.2.e en 5.1.2.e. Uit update van NCSC komt het overleg met DBB aan de orde. NCTV DBB is geinteresseerd, mede omdat er ook berichtgeving van een andere aanval bij een Europese dienstverlener is geweest. NCTV geeft aan dat ook gegevens van Rijksoverheid bij ID-ware zijn, maar heeft geen bron. Verder bespreken we het risico: voor de leden van de kamers is het risico lag vanwege de publieke rol die zij hebben en omdat er geen privé gegevens worden beheerd in het system. 5.1.2.e.
  TK heeft aan ID-ware gemeld dat NCSC namens hen acteert. Contactgegevens van woordvoering wordt uitgewisseld.

Zondag 2 oktober 2022

- 12:00 Overleg tussen 5.1.2.e, 5.1.2.e, 5.1.2.e, 5.1.2.e en 5.1.2.e, Hierbij is ook NCSC aangehaakt (vanuit response coördinatie). Situatie is ongewijzigd. Operationele coördinatie is overgedragen door 5.1.2.e aan NCSC. Van belang dat NCSC inschatting maakt van doelgroep, afstemmen woordvoeringslijn, ook voor de bestuurlijke lijn. NCSC geeft aan dat zij zelf nog geen contact hebben kunnen krijgen met IDWare, dat volgt pas na onderzoek door 5.1.2.f. Wel heeft Team High Tech Crime contact gelegd met IDWare. Via die weg ontvangt NCSC ook informatie. Er is een sprankje hoop dat de database met persoonsgegevens niet is geraakt. Wel zijn fileservers geraakt. Hier staan mogelijk ook persoonsgegevens in bestanden. Nog steeds is niet duidelijk of gegevens van de Eerste en Tweede Kamer bij zitten. Onderzocht wordt hoe data binnen het systeem stroomt. Er vindt monitoring plaats op darkweb en open bronnen. Er zijn nog geen aangeboden documenten aangetroffen van 1e en 2e Kamer. Er zijn o.a. 2 hoofdsites in beeld, deze zijn echter slecht te bereiken. 5.1.2.e heeft [illegible] en Staatssecretaris BZK geïnformeerd, TK heeft Voorzitter geïnformeerd. Rijkspas is niet bereikbaar voor 5.1.2.e : er wordt niet opgenomen. Dit is niet acceptabel. NCSC gaat kijken of zij een andere ingang hebben. NBV is nog niet ingeschakeld. Van belang dat dit tijdig gebeurt o.a. i.v.m. statelijke actoren. Voor nu is er nog geen toegevoegde waarde. Koppelvlak bij TK is geblokkeerd, bij het Rijk is dit nog niet het geval. Koppelvlakken worden door politie onderzocht, echter is dat nog geen technische onderzoek. TK heeft maandag overleg met IDWare over workaround m.b.t. mogelijkheid aanmaken nieuwe passen.
  De ransomware is een z.g. RAAS-variant, waardoor er twee actoren betrokken zijn: de aanbieder van het paltform voor ransomware en de actor die de campagne uitvoert. Het is nog niet bekend wie initiële actie heeft uitgezet. De aanbieder van het platform is waarschijnlijk een criminele organisatie zonder verbanden met statelijke actoren.
  NCTV en NCSC hebben vandaag nog overleg. Morgen (maandag) zal het onderwerp in het CIIC worden besproken tussen NCSC, AIVD, MIVD,Politie en OM en 5.1.2.e wordt hierover geïnformeerd en deze zet dit weer door als dit nodig is naar 1e en 2e Kamer. TK stelt Q&A op, dit vergt afstemming met NCSC. Voorafgaand aan eventuele informeren van pasgebruikers wordt dit afgestemd met de Dienst Bewaken & Beveiligen, met bijzondere aandacht voor DKDB. 5.1.2.b
  Ook zijn er nog veel open vragen (zie onder samenvatting gestelde vragen door TK in deze). Deze worden door NCSC opgepakt. Nogmaals is benadrukt dat er 1 lijn moet zijn voor communicatie.

- **Maandag 3 oktober later op de dag weer een gezamenlijk overleg 5.1.2.e plant deze.**
- **Inmiddels is overleg geplanned bij NCSC op maandagochtend om 11:00.**

Maandag 3 oktober 2022

11:00 Incidentoverleg bij NCSC: Alle betrokkenen vanuit de overheid zijn uitgenodigd voor het incidentoverleg met als doel het beeld compleet te krijgen en duidelijkheid te brengen over welke

lijnen er lopen. 5.1.2.e en 5.1.2.e van ID-ware geven eerst een toelichting. In detail wordt verteld hoe het verloop van de aanval is geweest, wanneer detectie heeft plaatsgevonden en hoe de respons van ID-ware is geweest. Herstel van de servers was mogelijk omdat een recente backup kon worden gebruikt. Geconstateerd is dat meer dan 200 Gb aan data is geëxfiltreerd. Er is geen betaling gedaan. ID-ware geeft aan dat het onderzoek een langdurige klus is vanwege het handwerk dat hiervoor nodig is. Ze verwachten eind deze week/begin volgende week uitsluitsel.

Afgesproken met ID-ware is dat er gemeenschappelijk overleg komt tussen ID-ware, 5.1.2.f en NCSC5.1.2.f . Ook dat woordvoering wordt afgestemd.

Daarna volgt overleg tussen alleen de overheidspartijen. THTC van politie licht haar bevindingen toe. In de tot nu toe (beperkte hoeveelheid) onderzochte gegevens zijn nog geen klantgegevens gevonden. Aangifte wordt dinsdagmiddag opgenomen. CISO Rijk meldt dat bevestigd is dat van 3500 medewerkers gegevens uit de thuisbezorgservice zijn gelekt. Het gaat om naam, rijkspasnummer en handtekening die gegeven is bij het afleveren. De betreffende organisatie is op de hoogte gesteld.

Er wordt gesproken over het risico van namaken van de pas en de mogelijkheid om toegang tot gebouwen te krijgen. Die kans is klein. Er wordt gesproken over het risico voor de VPN-verbindingen. Hierop is monitoring nodig (en inmiddels ingericht). Het bezit van sleutelmateriaal bij ID-ware is nihil, mogelijk dat paslezers die bij ID-ware in beheer zijn sleutelmateriaal bevatten. Dit moet worden nagegaan.

Het NCSC doet de centrale coördinatie richting ID-ware.

12:30 PO Staatssecretaris BZK met DGDOO. Korte mondelinge update aan stass door 5.1.2.e . Stass geeft aan snel te communiceren.

13:00 Beleidoverleg bij NCTV

Aanwezig zijn NCTV, woordvoering NCSC en JenV, NCSC, AIVD, 5.1.2.e Rijksoverheid. Het beeld wordt nog een keer gedeeld. Hier worden de verschillende scenario's besproken, de onderwerpen waar zekerheid over verkregen moet worden (aangifte, klantenlijst, behouden integriteit Rijkspas, behouden B67 als veilig gebied, analyse van de gelekte gegevens). Er moet duidelijkheid verkregen worden of ID-ware betrokken is bij Defensiepas (inmiddels bekend: niet). Er komt nog geen actie op DBB en Defentie.

Een aantal mogelijke handelingsperspectieven worden benoemd, naast de communicatiescenario's die al gedeeld waren: neem in inkoopvoorwaarden op dat NCSC namens het Rijk vragen mag stellen (langere termijn handeling) en bij de medewerkers van de servicedesks bewustzijn creëeren dat iemand mogelijk een pasnummer gebruikt om zich telefonisch te legitimeren, maar dat dat niet de bedoeling is (no-regret actie)

16:00 contact tussen Rijkspas (5.1.2.e , daarna 5.1.2.e) en 5.1.2.e . Vanwege vakantie en door gemiste oproepen 5.1.2.e was het nog niet gelukt contact te hebben. Wel is vanaf het vakantieadres intensief overleg geweest met ID-ware. Er was evenwel geen melding gedaan aan 5.1.2.e Vanmorgen is een impactanalyse gemaakt (om 13:00 gedeeld met 5.1.2.e), waaruit de 3500 gelekte adressen naar voren kwam. Rijkspas geeft aan dat het onderzoek nagenoeg compleet is afgerond en er geen andere persoonsgegevens zijn gevonden. Dit staat in contrast met het overleg van 11:00, waar ID-ware aangeeft nog bezig te zijn met het onderzoek.

17:30 Communicatieoverleg

Woordvoerders NCSC, JenV, BZK, EK en TK overleggen over de communicatieaanpak. Nog geen terugkoppeling ontvangen.

Er is geen **volgend overleg** geplanned. Indien er ontwikkelingen zijn stel ik voor dat we dinsdag eind van de dag even contact hebben. Ik zal daar een reservering voor uitsturen.

Dinsdag 4 oktober 2022

Terugkoppeling uit communicatieoverleg 3 oktober is dat de scenario's en actielijnen die zondag zijn opgesteld gevolgd gaan worden. Voor nu is het onderzoek van de gelekte files nog te onzeker om al te communiceren: kans is nog groot dat snel daarna opnieuw gecommuniceerd moet worden. Ook is de onzekerheid over mogelijk risico bij pasgebruikers voor hen te groot. Communicatieoverleg heeft de 3 triggers besproken, deze gelden nu nog niet.

17:00 Incidentoverleg tussen 5.1.2.e

Er zijn nog enkele leads vanuit TK gedeeld met NCSC. Onder meer mogelijk lekken van persoonsgegevens via logfiles. Vooralsnog geen veranderingen in de situatie. Het onderzoek naar de gelekte gegevens loopt nog. Woordvoerders worden aan woordvoering NCSC gekoppeld. Morgen is het commissiedebat Digitaliserende Overheid. Voor mogelijke vragen over ID-ware wordt de woordvoeringslijn gehanteerd die we hebben opgesteld.

Woensdag 5 oktober 2022

Commissiedebat Digitaliserende Overheid: de hack bij ID-ware is niet aan de orde geweest. Gesproken met 5.1.2.e . Zij maakt er zich zorgen over dat ongenuanceerde berichtgeving vanuit de Rijksoverheid zeer veel schade toebrengt. Aangegeven dat we de nuance steeds aanbrengen, maar dat harde resultaten dat er niets gebeurdis ons nog niet bereikt hebben. 5.1.2.e geeft aan dat het conceptrapport van 5.1.2.f donderdagochtend gedeeld zal worden en het definitieve rapport vrijdag.

17:00 – 18:15 Bestuurlijk overleg bij NCTV met NCSC

Het beeld weer aangevuld en de risico's afgepeld. 5.1.2.f

De duiding is dat de risico's voor medewerkers en toegang tot gebouwen (5.1.2.f bekend en te overzien zijn. Mogelijke nieuwe feiten zullen hier niet veel meer aan veranderen. Morgenochtend komen er resultaten beschikbaar via een conceptrapport van 5.1.2.f. Als dit geen heel ander beeld oplevert is het tijd om te gaan communiceren, in de volgorde eerst intern (Rijksoverheid, Eerste en Tweede Kamer), dan vanuit de stass naar de Kamers. NCSC informeert ook haar doelgroepen (incl. vitaal). Coördinatie van de timing verloopt via het overleg van woordvoerders. Bekend is dat bij pashouders van de TK ook journalisten zijn, waarvan sommigen geen e-mailadres bekend is. Alle pasgebruikers van EK en TK krijgen daarom een brief.

Donderdag 6 oktober 2022

Het conceptrapport van 5.1.2.f wordt via NCSC gedeeld. De onderzoeksmethode staat beschreven, maar niet dat alle data die gelekt is onderzocht is. Nog steeds bestaat de mogelijkheid dat er persoonsgegevens tussen zitten. TK heeft NCSC voorzien van nieuwe links naar gelekte gegevens. NCSC heeft moeite om de gegevens vanaf de leak site te downloaden, dit gaat nog dagen duren voordat alles er is, mogelijk nog weken voordat alles doorgespit is.

Mensen van de beveiligingsorganisaties (BVA's en CISO's) zijn geïnformeerd met het verzoek nog niet verder te communiceren.

Rijkspasbeheer heeft op eigen initiatief en zonder overleg met woordvoerders op Intranet gecommuniceerd.

Woordvoerders hadden gepland op maandag een brief naar de kamer te sturen. Stass BZK wil nog donderdagavond. Besloten wordt vrijdag ochtend te communiceren, omdat eerst de medewerkers op de hoogte gebracht. Brief van stass aan TK is in concept opgesteld en afgestemd met EK, TK, BVA Rijk, NCSC en Rijkspasbeheer. Wijzigingen doorgevoerd en de lijn ingestuurd met het verzoek de brief te sturen nadat EK, TK en RO gelegenheid hebben gehad intern te communiceren.

Vrijdag 7 oktober 2022

Communicatie via portalen en bericht verloopt in de ochtend. De Volkskrant heeft als eerste een artikel, andere media volgen. Rond het middaguur worden de brief aan de TK en de nota gepubliceerd. Na de MR staat de stass de pers te woord. Ook EK krijgt een brief. Ondanks dat

berichtgeving wat ongenuanceerd is, blijft de toon in de media redelijk neutraal. Alleen Telegraaf maakt er een spannend verhaal dat informatie via een gelekt e-mailbericht is binnengekomen.

Zaterdag 8 oktober 2022

ID-ware heeft ook een bericht gepubliceerd Incident Statement (id-ware.com). Daarin "*For confidentiality reasons, ID-ware cannot provide details about its individual customers. However, ID-ware can confirm that the investigation to date has not revealed any evidence that data of members of parliament or other public figures in the Netherlands was affected by data leakage.*" Dit leidt weer tot onduidelijkheid: heeft de stass de Kamer dan verkeerd ingelicht? ID-ware stelt dat onderzoek tot nu tot niet heeft aangetoond dat gegevens van kamerleden of publieke figuren zijn gelekt. Dat is ook niet wat de stass heeft gezegd. Wat ID-ware niet zegt is dat er 3487 namen gelekt zijn van de Rijksoverheid, wat de stass als enige juist wel noemt. En wat bevestigd is door ID-ware en Fox-IT.

Ook meldt 5.1.2.e in niet mis te verstane woorden dat het bericht op Rijksportaal, waarin staat dat ID-ware Rijkspassen levert tot onvoorstelbare schade leidt.

Zondag 9 oktober 2022

Rustige dag, op een 'persoonlijk memo' van 5.1.2.e aan CIO Rijk na.

16

5.1.2.e

Van: 5.1.2.e (NCSC-NL) <5.1.2.e @ncsc.nl>
Verzonden: maandag 10 oktober 2022 08:29
Aan: 5.1.2.e
Onderwerp: RE: Bijgewerkte tijdlijn

[TLP:AMBER]

Dag 5.1.2.e

Dank, we checken het stuk vandaag nog even.

Wellicht is er nog een kort afstemmingsoverleg nodig tussen 5.1.2.e en NCSC. Er zijn nog enkele vragen binnen gekomen vanuit de departementen.

5.1.2.e

From: 5.1.2.e <5.1.2.e @minbzk.nl>
Sent: zondag 9 oktober 2022 23:03
To: 5.1.2.e 5.1.2.e k@minbzk.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @eerstekamer.nl>; 5.1.2.e <5.1.2.e @ncsc.nl>
Subject: Bijgewerkte tijdlijn

Beste collega's,

Bijgaand een bijgewerkte tijdlijn van het ID-ware incident. Als jullie nog opmerkingen of aanvullingen hebben hoor ik ze graag. Vooralsnog zijn er geen nieuwe acties. Als het nog nodig is plannen we nog een incidentoverleg, en anders plan ik graag een evaluatie met jullie.

Groet,

5.1.2.e

5.1.2.e

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Directie CIO Rijk | DG Overheidsorganisatie
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20011 | 2500 AE | Den Haag
e-mail: 5.1.2.e @minbzk.nl
telefoon secretariaat: 5.1.2.e | mobiel: 5.1.2.e

Factsheet en tijdlijn ID-ware hack tbv mondelinge vragenuur

Wat is er gelekt?
De gegevens die gelekt zijn, lijken afkomstig uit een database waarin gegevens waren opgeslagen van personen die de rijkspas thuis opgestuurd zouden krijgen. Dit gaat om medewerkers van de rijksoverheid, de Eerste Kamer en de Tweede Kamer. Voor de laatste twee geldt dat dit om de gehele organisatie gaat, en niet enkel de Kamerleden zelf. Op het moment is zicht op ongeveer 3500 personen om wie het zou gaan (werkzaam bij de Belastingdienst). Op het moment zijn daar voor zover bekend geen Eerste of Tweede Kamerleden zelf bij.

Onduidelijkheid hierover
In de berichtgeving over de Kamerbrief (zie ook mediaoverzicht), gaven sommige media, onder meer de Volkskrant en Telegraaf, onjuist weer dat er gegevens van Kamerleden gelekt zouden zijn. De Volkskrant schrijft dit onjuist in de kop van het artikel op 7 oktober, maar gaat er in het artikel niet op in. De Telegraaf heeft de email gezien die de BVA/CISO Tweede Kamer aan iedereen werkzaam binnen die organisatie heeft gestuurd op vrijdag, om hen te informeren over het lek. Dat is dus naar zowel de Kamerleden als alle medewerkers.

ID-ware statement
Statement ID-ware 7 oktober
Naar aanleiding van de deels onjuist berichtgeving, heeft ID-ware op 7 oktober een incident statement uitgebracht (zie bijlage 4d). Dit statement is niet afgestemd met de overheid. In het statement beschrijft men kort wanneer men achter het incident kwam, en wat men sindsdien gedaan heeft. Ook betuigt men spijt over het incident, en wordt de samenwerking met de overheid benoemd. Het statement meldt in reactie op de berichtgeving twee belangrijke punten:

1) Het statement stelt dat "ID-ware kan bevestigen dat uit onderzoek tot op heden niet is gebleken dat er data van Kamerleden of andere publieke personen bij het datalek betrokken zijn." Dit statement komt voor rekening van ID-Ware, en kunt u niet bevestigen of ontkennen. Wat u heeft aangegeven aan de Kamer is dat er ongeveer 3500 namen zijn gelekt. Dat aantal is bevestigd in ID-Ware in contact met de overheid, en ook door 5.1.2.f die het onderzoek doen. Ambtenaren, wiens gegevens gelekt zijn, zijn werkzaam in het publieke domein.

2) Het statement stelt verder dat de aanval zou zijn uitgevoerd door de bekende ransomware groep BlackCat, ook bekend als AHLPV. In verband met het nog lopende onderzoek van onder andere de politie, kunt u deze stelling niet bevestigen of ontkennen.

Dit statement was ook aanleiding voor media-berichtgeving, maar minder dat de kamerbrief op 7 oktober. Over het statement van ID-Ware hebben de Volkskrant, het Nederlands Dagblad, RTL nieuws, security.nl en PZC gepubliceerd.

Stand van zaken onderzoeken

- Het NCSC monitort welke gelekte data op internet (bijvoorbeeld het darkweb) beschikbaar wordt gesteld. Die data kan dan worden geanalyseerd, ten behoeve van onder meer de medewerkers in kwestie. Dit kan nog enige tijd.
- Vanuit de Nationale Politie wordt er ook gekeken, vanuit eventuele strafrechtelijke blik. Hierover kunnen publiekelijk geen nadere uitspraken worden gedaan.
- Het incident bij ID-ware en de gevolgde procesgang zal, zoals gebruikelijk bij incidenten, geëvalueerd worden door betrokken partijen ook CIO Rijk. Zodoende kunnen daar lessen van geleerd worden en waar nodig processen worden verbeterd.

Al deze onderzoeken en evaluaties zullen een doorlooptijd hebben van weken zo niet maanden. De Kamer zal vanwege de vertrouwelijkheid heir niet altijd in detail over geïnformeerd kunnen worden. Wel kunt u aangeven dat u de Kamer indien noodzakelijk verdere updates zult sturen.

Tijdlijn

- 17/18 september: ransomware aanval op ID-ware, persoonsgegevens zijn buitgemaakt.
- 21 september: op basis van melding ID-ware bij Tweede Kamer heeft CISO Tweede Kamer contact met CISO Rijk. Er loopt op dat moment een onderzoek van 5.1.2.f naar het incident, in opdracht van ID-ware.
- 30 september: ID-ware heeft een brief gestuurd aan de TK. Het is dan duidelijk dat er veel bestanden zijn gelekt via een bericht op Darkweb. TK heeft dan een operationeel crisisteam ingericht. Tweede en Eerste Kamer hebben melding gedaan bij Autoriteit Persoonsgegevens.

- CISO Rijk neemt contact op met NCSC. NCSC was wel al bekend met een mogelijke aanval op ID-ware, maar had nog geen melding gekregen. CISO Rijk geeft aan dat deze melding mede namens TK is. In het overleg wordt de tot nog toe bekende informatie uitgewisseld en contactinformatie voor het weekend gedeeld.
- 1 oktober: overleggen tussen BVA's TK en eK en CISO Rijk. CISO Rijk pakt op verzoek van hen regie. Het NCSC pakt vanuit zijn rol coördinatie onder meer met de Nationale Politie.
- 2 oktober: operationale coördinatie is overgedragen aan het NCSC. StassBZK en DGDOO zijn door CISO Rijk geïnformeerd. Op zondag 2 oktober om 12.00 uur zijn er op darkweg nog geen aangeboden documenten van TK en EK gevonden.
- 3 oktober: incidentoverleg bij het NCSC, met ID-ware aanwezig. ID-ware licht het incident en respons toe. ID-ware heeft geen betaling gedaan richting de actor.
- 3 oktober: CISO Rijk kan melden in het incident overleg dat van 3500 medewerkers gegevens uit de thuisbezorgservice zijn gelekt. Het gaat om naam, rijkspasnummer en handtekening.
- 3 oktober: in PO StasBZK – DGDOO wordt er korte mondelinge update gegeven, en afgesproken spoedig de Kamer te informeren.
- 3 oktober: naast operationeel overleg ook beleidsoverleg onder coördinatie NCTV.
- 4 oktober: operationeel overleg, maar geen nieuwe ontwikkelingen. Contact over woordvoering tussen o.a. BZK, JenV en Eerste en Tweede Kamer loopt.
- 5 oktober: bestuurlijk overleg, waarbij wordt afgesproken spoedig Kamer te informeren, op basis van het te ontvangen concept-rapport 5.1.2.f.
- 6 oktober: conceptrapport 5.1.2.f via het NCSC ontvangen. Duidelijk is dat het een tijd zal duren voordat alle gelekte informatie gevonden en doorzocht is op persoonsgegevens. BVA's en CISO's zijn geïnformeerd. Een concept-Kamerbrief wordt na afstemming ter akkoord aan StasBZK voorgelegd.
- 7 oktober: getroffen medewerkers worden via verschillende kanalen geïnformeerd. de Kamerbrief wordt verzonden, wat leidt tot media-aandacht.
- 8 oktober: ID-ware publiceert een statement.
- 10 oktober: geen operationele of bestuurlijke overleggen meer. Onderzoeken vanuit o.a. NCSC en politie lopen. Mondelinge vraag van D66 wordt aangemeld.

18

5.1.2.e

Van: 5.1.2.e <5.1.2.e @minjenv.nl>
Verzonden: donderdag 10 november 2022 17:22
Aan: NCSC Bestuurlijke Ondersteuning; 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: Kamerbrief update hack bij ID-ware - Tweede Kamer

Hi 5.1.2.e en anderen,
De sondering loopt idd via de PA's. De motie over het DTC voor het WGO van maandag a.s. wordt door EZK opgepakt en met ons afgestemd. Wij stemmen met het NCSC hierover af net als voor evt andere voor ons relevante moties of vragen voor het WGO.
De aangepaste brief is door BZK niet meer met ons afgestemd. Zouden jullie dat in het vervolg wel willen doen? (volgens mij ook eerder verzocht?)
Alvast dank!
Gr,
5.1.2.e

Van: NCSC Bestuurlijke Ondersteuning <ncsc.bestuurlijke.ondersteuning@ncsc.nl>
Verzonden: donderdag 10 november 2022 17:04
Aan: '5.1.2.e' <5.1.2.e @minbzk.nl>; 5.1.2.e <n5.1.2.e @ncsc.nl>
CC: 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @minjenv.nl>; 5.1.2.e <5.1.2.e @minjenv.nl>; 5.1.2.e <5.1.2.e @minjenv.nl>; 5.1.2.e <5.1.2.e @minjenv.nl>; 5.1.2.e <5.1.2.e @minjenv.nl>
Onderwerp: RE: Kamerbrief update hack bij ID-ware - Tweede Kamer

Hoi 5.1.2.e en anderen in cc,

Dank voor je reactie. Ik begrijp dat je 5.1.2.e inmiddels ook hebt gesproken en dat jullie gezamenlijke conclusie was dat 5.1.2.e met 5.1.2.e moest bellen. Dat gesprek heeft zojuist in goede harmonie plaatsgevonden.

5.1.2.i/5.2.1

Voor volgende brieven en/of andere parlementaire afstemming worden we graag eerder en nauwer betrokken.

Gr 5.1.2.e

Van: 5.1.2.e <5.1.2.e @minbzk.nl>
Verzonden: donderdag 10 november 2022 16:19
Aan: NCSC Bestuurlijke Ondersteuning <5.1.2.e @ncsc.nl>
CC: 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @minjenv.nl>; 5.1.2.e <5.1.2.e @minjenv.nl>; 5.1.2.e <5.1.2.e @minjenv.nl>
Onderwerp: RE: Kamerbrief update hack bij ID-ware - Tweede Kamer

Hallo 5.1.2.e,

Om te beginnen met je laatste vraag eerst: de sondering voor het debat maandag loopt nu via de verschillende PA's. Dat wordt dan al doorgeleid naar het departement dat er over gaat. Ik zag een en ander langskomen in relatie tot DTC, maar dat is richting EZK gegaan. Pakken we vanuit BZK niet op.

Qua ID-ware brief: deze ligt inmiddels bij de staatssecretaris, dus de reactie moeten we ter kennisgeving aannemen in dit geval denk ik. Enkele van je inhoudelijke vragen kan ik helaas niet beantwoorden, omdat ik daarvoor niet nauw genoeg bij ID-ware betrokken was.

Groet,
5.1.2.e

Van: 5.1.2.e <5.1.2.e @ncsc.nl>
Verzonden: donderdag 10 november 2022 15:53
Aan: 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @ncsc.nl>
CC: 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @minjenv.nl>; 5.1.2.e <5.1.2.e @minjenv.nl>; 5.1.2.e <5.1.2.e @minjenv.nl>
Onderwerp: RE: Kamerbrief update hack bij ID-ware - Tweede Kamer

Hoi 5.1.2.e,

Zie bijgaand enkele suggesties, vragen en opmerkingen vanuit het NCSC. Wat ik eigenlijk nog een beetje mis in de brief zijn de contractuele afspraken met ID-ware (en evt. andere leveranciers van Rijksoverheid, Tweede- en Eerste Kamer) en de waarborgen die we daarin laten opnemen.

Zijn er verder nog zaken in de voorbereiding op het debat van maandag waar we naar moeten/kunnen kijken?

Gr 5.1.2.e

Van: 5.1.2.e <5.1.2.e @minbzk.nl>
Verzonden: donderdag 10 november 2022 10:35
Aan: 5.1.2.e <5.1.2.e @ncsc.nl>
CC: 5.1.2.e <5.1.2.e @minbzk.nl>
Onderwerp: Kamerbrief update hack bij ID-ware - Tweede Kamer

Hallo 5.1.2.e,

Naar aanleiding van jouw berichtje vanochtend bijgevoegd de nieuwe versie van de Kamerbrief ID-ware, zoals die nu bij DGDOO ter akkoord ligt. Verzending is voorzien voor het weekend, met het oog op het debat maandag.

Groet,
5.1.2.e

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

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Ministry of Justice and Security

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

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Ministry of Justice and Security

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

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Ministry of Justice and Security

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

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Ministry of Justice and Security

19

5.1.2.e

Van: 5.1.2.e <5.1.2.e @ncsc.nl>
Verzonden: donderdag 20 oktober 2022 11:28
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: Update ransomware-aanval ID-ware

Beste allen,

Zoals eerder bericht is het NCSC niet meer opgeschaald voor deze casus. Dit betekent niet dat er geen aandacht voor deze casus is. Als er relevante vragen/zaken zijn, dan verzoek ik jullie de CERT-box te mailen (cert@ncsc.nl). Het CERT/Fusion Center kan dan verder actie ondernemen.

Groeten,

5.1.2.e
Nationaal Cyber Security Centrum
.....
Ministerie van Justitie en Veiligheid
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20011 | 2500 EA | Den Haag
.....
T + 5.1.2.e
E 5.1.2.e @ncsc.nl

From: 5.1.2.e <5.1.2.e @minbzk.nl>
Sent: donderdag 20 oktober 2022 10:54
To: 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @ncsc.nl>
Cc: 5.1.2.e @eerstekamer.nl' <5.1.2.e @eerstekamer.nl>
Subject: RE: Update ransomware-aanval ID-ware

5.1.2.e zal contact zoeken met jou want als er EK-pashouders tussenzitten dan bepalen wij als EK zelf hoe en door wie richting EK-pashouders gecommuniceerd wordt. Lijkt nu een autonoom proces zonder ons, wij wisten hier ook niet eerder van vanuit Rijksdienst ed.

Met vriendelijke groet,

5.1.2.e
DG Digitalisering en Overheidsorganisatie (DGDOO)
.....
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20011 | 2500 EA | Den Haag
.....
T + 5.1.2.e
E 5.1.2.e @minbzk.nl

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Datum: donderdag 20 okt. 2022 10:33 AM
Aan: 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>, 5.1.2.e)' <5.1.2.e @ncsc.nl>
Kopie: 5.1.2.e @eerstekamer.nl' 5.1.2.e @eerstekamer.nl>
Onderwerp: RE: Update ransomware-aanval ID-ware

Beste allen,

De TK heeft gisteren van ID-Ware een bestand gekregen met daarop ongeveer 1300 namen van onze pashouders. Dit bestand is gedeeld met onze FG en met onze rijkspasautoriteit 5.1.2.e Wij moeten nog onderzoeken wie de genoemde personen zijn, wie van EK is en van TK, etc. Vervolgens moet worden bepaald of en, zo ja, op welke wijze de betrokkenen worden geïnformeerd.

5.1.2.e

5.1.2.e
Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA
+5.1.2.e
T 5.1.2.e | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

-----Oorspronkelijk bericht-----
Van: 5.1.2.e <5.1.2.e @minbzk.nl>
Verzonden: donderdag 20 oktober 2022 10:27
Aan: 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @ncsc.nl>
CC: 5.1.2.e @eerstekamer.nl' <5.1.2.e @eerstekamer.nl>
Onderwerp: RE: Update ransomware-aanval ID-ware

Snap hier niks van.bij de EK is dit niet bekend hoor.

Met vriendelijke groet,

5.1.2.e
.....
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties Turfmarkt 147 | 2511 DP | Den Haag Postbus 20011 | 2500 EA | Den Haag .....
T 5.1.2.e
E 5.1.2.e @minbzk.nl

Van: 5.1.2.e <5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>
Datum: donderdag 20 okt. 2022 9:00 AM
Aan: 5.1.2.e <5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>, 5.1.2.e <5.1.2.e @tweedekamer.nl<mailto:5.1.2.e @tweedekamer.nl>>, 5.1.2.e <5.1.2.e @ncsc.nl<mailto:5.1.2.e @ncsc.nl>>
Onderwerp: FW: Update ransomware-aanval ID-ware

Ter info,

Groet,

5.1.2.e
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties Directie CIO Rijk | DG Digitalisering en Overheidsorganisatie
Turfmarkt 147 | 2511 DP | Den Haag .....
e-mail: 5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>
mobiel: 5.1.2.e | telefoon secretariaat: 5.1.2.e

Van: 5.1.2.e <5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>
Datum: donderdag 20 okt. 2022 8:56 AM
Aan: 5.1.2.e <5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>, 5.1.2.e 5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>, 5.1.2.e 5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>
Onderwerp: RE: Update ransomware-aanval ID-ware

Ha 5.1.2.e

Dank voor de update, dit was eerder bekend maar toen ontkent. Welk onderzoek heeft dit nu bevestigd? Komt dit van 5.1.2.f of ID-ware zelf? Wil je me de communicatie doorsturen?

Groet,

5.1.2.e

5.1.2.e
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties Directie CIO Rijk | DG Digitalisering en Overheidsorganisatie
Turfmarkt 147 | 2511 DP | Den Haag .....
e-mail: 5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>
mobiel: 5.1.2.e | telefoon secretariaat: 5.1.2.e

Van: 5.1.2.e 5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>
Datum: woensdag 19 okt. 2022 3:56 PM
Aan: 5.1.2.e 5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>, 5.1.2.e <5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>, 5.1.2.e <5.1.2.e @minbzk.nl<mailto:5.1.2.e @minbzk.nl>>
Onderwerp: RE: Update ransomware-aanval ID-ware

Goedemiddag,

N.a.v. recent verkregen informatie weer een korte update:

* Van ca. 1300 personen uit de EK/TK-populatie zijn persoonsgegevens gelekt, verkregen uit het 5.1.2.f
* De EK/TK is hierover door ID-ware en NCSC geïnformeerd en op de hoogte gesteld om welke data het gaat;
* Het is aan de EK/TK om betrokkenen te informeren;
* 5.1.2.f heeft haar definitieve onderzoeksrapport nog niet opgeleverd. Aanvullend is een samenvatting gevraagd mbt rijksoverheid bevindingen.

Vriendelijk groet,

5.1.2.e

Van: 5.1.2.e
Verzonden: dinsdag 11 oktober 2022 17:15
Aan: 5.1.2.e 5.1.2.e @minbzk.nl>; 5.1.2.e 5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>
Onderwerp: Update ransomware-aanval ID-ware

Beste allen,

Een korte update m.b.t de ransomware-aanval bij ID-ware:

* NCSC heeft ID-ware vanmiddag op de hoogte gesteld dat in een applicatie logbestand persoonsgegevens van de Eerste en Tweede Kamer populatie zijn aangetroffen;
* Om hoeveel personen en welke gegevens het betreft wordt momenteel onderzocht. ID-ware verwacht daar morgen meer info over te krijgen van NCSC;
* ID-ware heeft contact opgenomen met CISO Tweede Kamer en hiervan melding gemaakt.

Voor alle duidelijkheid: het betreft dus alleen gegevens van de EK/TK, aangezien alleen zij gebruik maken van 5.1.2.f van ID-ware.

M.b.t de gelekte thuisbezorg afleverbewijzen Belastingdienst:

* Het betreft 3195 afleverbewijzen (i.t.t het eerder genoemde aantal van 3500).
* Betrokken medewerkers zijn/worden door de BD geïnformeerd.

Vriendelijk groet,

5.1.2.e

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.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

20

5.1.2.e

Van: 5.1.2.e
Verzonden: dinsdag 25 oktober 2022 14:45
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: Vragen Stas ransomware-aanval ID-ware
Bijlagen: Buiten reikwijdte

5.1.2.e ,

Bijgaand de versie van vandaag. Laat me weten als je op- of aanmerkingen hebt.

Groet,

5.1.2.e

Van: 5.1.2.e @minbzk.nl>
Verzonden: maandag 24 oktober 2022 18:20
Aan: 5.1.2.e @minbzk.nl>
CC: 5.1.2.e @minbzk.nl>; 5.1.2.e @minbzk.nl>
Onderwerp: RE: Vragen Stas ransomware-aanval ID-ware

Beste 5.1.2.e ,

Ik kreeg (vanuit jouw team) een verzoek om in gesprek te gaan over 'vragen van de Stas' waaruit ik heb afgeleid dat er mogelijk nieuwe vragen zijn binnengekomen.
Hieruit blijkt maar weer dat we elkaar moeten blijven informeren en samenwerken (met de mensen die hierin een rol hebben), om misinterpretatie te voorkomen en een juist beeld te geven van de stand van zaken en impact.
Naar de Kamer, bij vragen van de media alsook in onze interne communicatie binnen de rijksoverheid.
In dat kader wil ik je vragen om mij te betrekken in de Q&A die wordt opgesteld voor het debat van 2 november.

Alvast dank en een fijne avond.

Met vriendelijk groet,

5.1.2.e

Van: 5.1.2.e <5.1.2.e @minbzk.nl>
Verzonden: maandag 24 oktober 2022 17:31
Aan: 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>
CC: 5.1.2.e <5.1.2.e @minbzk.nl>
Onderwerp: RE: Vragen Stas ransomware-aanval ID-ware

Ha 5.1.2.e ,

Als je doelt op de vragen n.a.v. het persbericht van ID-ware op zaterdag 8 oktober: die zijn ter voorbereiding op mogelijke mondelinge vragen op dinsdag 11 oktober al beantwoord door 5.1.2.e , zie bijgaand. Ik ben me niet bewust van nieuwe vragen. Wel houden we rekening met vragen tijdens het debat van 2 november, hiervoor wordt een Q&A voorbereid, met dezelfde strekking. Over de 1300 gelekte gegevens van EK en TK putten we uit jouw bericht waarin dit wordt bevestigd.

Groet,

5.1.2.e

Van: 5.1.2.e <5.1.2.e @minbzk.nl>
Verzonden: maandag 24 oktober 2022 14:17
Aan: 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>
CC: 5.1.2.e 5.1.2.e @minbzk.nl>
Onderwerp: Vragen Stas ransomware-aanval ID-ware

Beste 5.1.2.e,

Ik heb begrepen dat er vanuit de Stas vragen zijn gesteld over de ransomware-aanval op ID-Ware.

Kun je mij graag asap de vragen sturen zodat we deze juist en volledig kunnen beantwoorden?

Vriendelijk groet,

5.1.2.e

5.1.2.e

Van: 5.1.2.e
Verzonden: donderdag 27 oktober 2022 14:50
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: Debat 2 november -stasBZK
Bijlagen: Buiten reikwijdte

Hierbij de versie zoals zojuist telefonisch besproken

met vriendelijke groet,

5.1.2.e
5.1.2.e

Van: 5.1.2.e
Verzonden: donderdag 27 oktober 2022 13:24
Aan: 5.1.2.e <5.1.2.e @minbzk.nl>
CC: 5.1.2.e <5.1.2.e @minbzk.nl>
Onderwerp: FW: Debat 2 november -stasBZK

Beste 5.1.2.e,

Wij zijn nog met de update van de QA's bezig. Er volgt nog een nieuwe versie vanmiddag (mijn doel is uiterlijk 15 uur)

met vriendelijke groet,

5.1.2.e

Van: 5.1.2.e <5.1.2.e @minbzk.nl>
Verzonden: vrijdag 21 oktober 2022 15:46
Aan: 5.1.2.e <5.1.2.e @minbzk.nl>
CC: 5.1.2.e <5.1.2.e @minbzk.nl>
Onderwerp: RE: Debat 2 november -stasBZK
5.1.2.e,

Bijgevoegd de conceptstukken voor ID-ware. Aangezien dit onderwerp nog in ontwikkeling is, is voor het debat nog een update hierover nodig. Voor nu is dit de gegevens zoals we die hebben.

Groet,
5.1.2.e

Van: 5.1.2.e <5.1.2.e @minbzk.nl>
Verzonden: donderdag 20 oktober 2022 12:55
Aan: 5.1.2.e <5.1.2.e @minbzk.nl>
Onderwerp: RE: Debat 2 november -stasBZK

Ha 5.1.2.e,

Ik heb per abuis een ander schema naar jou gemaild, foutje!

hieronder tref je de juiste aan:

21 okt	Bespreking dossier in MT DGDOO. Dossier tevens via digidoc naar BA
18-21 okt	Tweede ronde - Afstemmen dossier met relevante BZK onderdelen (o.a. CZW, CIO-Rijk, DenB) en relevante departementen (o.a. JenV en EZK)
19-26 okt	Sondering en check op mediaberichten
24- 27 okt	Indien nodig aanvullen dossier op basis van opmerkingen MT DGDOO, BA, sondering en mediaberichten
27 okt	Definitieve dossier de lijn in richting stas BZK
31 okt	9.15-10.00 uur: bespreking dossier tijdens PO
1 nov	Indien nodig gezamenlijke voorbespreking stas BZK met min Rb
2 nov	Debat van 14.15 tot 18.15 uur

Met vriendelijke groet,

5.1.2.e

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Directoraat-Generaal Overheidsorganisatie
Directie Digitale Overheid
Turfmarkt 147 | 2511 DP | DEN HAAG
+5.1.2.e | 5.1.2.e @minbzk.nl

Van: 5.1.2.e <5.1.2.e @minbzk.nl>
Verzonden: donderdag 20 oktober 2022 12:51
Aan: [redacted] <5.1.2.e @minbzk.nl>
Onderwerp: RE: Debat 2 november -stasBZK

5.1.2.e,

Ik ben nu even naar de planning aan het kijken. 5.1.2.i/5.2.1 [redacted] Klopt die planning aan het einde?

Groet,
5.1.2.e

Van: 5.1.2.e <5.1.2.e @minbzk.nl>
Verzonden: donderdag 20 oktober 2022 10:38
Aan: 5.1.2.e <5.1.2.e @minbzk.nl>
Onderwerp: RE: Debat 2 november -stasBZK

Ha 5.1.2.e,

Dank voor je mails.
Wij zien je input tegemoet.

En als je een naam hebt van die CISO collega dan hoor ik het graag. Betekent dit trouwens dat degene dan met ons in de ambtenaren kamer in de TK aanwezig zal zijn?

Groet,

5.1.2.e

Verzonden met BlackBerry Work(www.blackberry.com)

Van: "5.1.2.e " <5.1.2.e @minbzk.nl>
Verzonden: 20 okt. 2022 10:30
Naar: "5.1.2.e " <5.1.2.e @minbzk.nl>
Cc: "5.1.2.e " <5.1.2.e @minbzk.nl>; "5.1.2.e " <5.1.2.e @minbzk.nl>; postbuspolitiekbestuurlijkCIORijk@minbzk.nl
Onderwerp: RE: Debat 2 november -stasBZK

Nog vergeten te beantwoorden: op het moment is 5.1.2.e degene met de meeste detailkennis over het incident. Ik zal zorgen dat hij beschikbaar is; ik heb niet de kennis om de staatssecretaris ter plekke van antwoorden te kunnen voorzien.

Groet,
5.1.2.e

Van: 5.1.2.e <5.1.2.e @minbzk.nl>
Verzonden: woensdag 19 oktober 2022 15:40
Aan: 5.1.2.e <5.1.2.e @minbzk.nl>
CC: 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>
Onderwerp: Debat 2 november -stasBZK
Urgentie: Hoog

Ha 5.1.2.e ,

Uit de mail van 5.1.2.e maak ik op dat er een onderwerp aan de convocatie is toegevoegd over de brief 'Hack bij ID-ware'.
Ben jij daarvoor de dossierhouder? Zo ja, ik heb voor het dossier van de stas daarover een factsheet nodig en 3 Q&A's voor haar dossier. Zie de bijlage voor de formats.
Toevallig was vandaag de deadline om het dossier naar het MT Digitaal te krijgen dus kunnen jouw stukken daar helaas niet meer in mee. Maar dat moet wel lukken voor als het dossier naar de stasBZK gaat.
Deadline voor aanleveren, factsheet en Q&A's: ***Vrijdag 21 oktober.***

Ik vroeg mij af, wie aanwezig zal zijn in de TK om de mogelijke vragen hierover te beantwoorden voor de stas.
Het gaat dit keer via de kamerdebatapp, dus het vergt wel enige training. Bijgevoegd daarom een korte handleiding.

Ons schema tot 2 november ziet er trouwens als volgt uit:

Woensdag 19 oktober	DS verwerkt input + lijn in (Digidoc)
Vrijdag 21 oktober	StasBZK – schriftelijke reactie op concept antwoord
Maandag 24 oktober	Verwerken evt. input stasBZK + Shaif mailt alle betrokken ministeries ter afstemming. Deadline (vrijdag 28 oktober)

Maandag 31 oktober	DS verwerkt evt. input ministeries
Dinsdag 1 november	Opstellen nota voor stasBZK
Woensdag 2 november	Deadline voor aanleveren Digidoc – stas moet uiterlijk 8 november getekend hebben

Mijn werktelefoon is helaas offline. Ik wacht op een nieuwe simkaart. Daarom graag per mail mij benaderen. Dank voor het begrip!

Met vriendelijke groet,

5.1.2.e

.....

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Directoraat-Generaal Overheidsorganisatie
Directie Digitale Overheid
Turfmarkt 147 | 2511 DP | DEN HAAG
5.1.2.e | 5.1.2.e @minbzk.nl

Van: 5.1.2.e <5.1.2.e @minbzk.nl>
Verzonden: woensdag 19 oktober 2022 14:59
Aan: 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>
Onderwerp: RE: Besluiten PV DiZa 19 oktober 2022

Hi 5.1.2.e,

Goed te weten.

Debat 2 november wordt voorbereid door DS, 5.1.2.e

Buiten reikwijdte

Groetjes,

5.1.2.e

Van: 5.1.2.e <5.1.2.e @minbzk.nl>
Verzonden: woensdag 19 oktober 2022 14:55
Aan: 5.1.2.e <5.1.2.e @minbzk.nl>
Onderwerp: FW: Besluiten PV DiZa 19 oktober 2022

Hallo 5.1.2.e,

Buiten reikwijdte

Groet,
5.1.2.e

Van: 5.1.2.e @minbzk.nl <5.1.2.e @minbzk.nl>
Verzonden: woensdag 19 oktober 2022 14:49
Aan: 5.1.2.e <5.1.2.e @rijksoverheid.nl>; 5.1.2.e <5.1.2.e @rijksoverheid.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @rijksoverheid.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @rijksoverheid.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>
CC: 5.1.2.e <5.1.2.e @minbzk.nl>
Onderwerp: Besluiten PV DiZa 19 oktober 2022

Beste allemaal,

Vanmorgen was de procedurevergadering commissie 5.1.2.e Er zijn een paar belangrijke besluiten genomen.

Toegevoegd aan agenda WGO van 14 november:

Buiten reikwijdte

Toegevoegd aan commissiedebat Bescherming Persoonsgegevens en digitale grondrechten van 2 november 2022

- Hack bij ID-ware

Buiten reikwijdte

Brieven zijn bijgevoegd!

Hartelijke groet
5.1.2.e

22

5.1.2.e

Van: 5.1.2.e
Verzonden: vrijdag 11 november 2022 15:54
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: Status ID-ware en uitwerking evaluatiesessie 1 november

5.1.2.e,

Dank voor al je acties en coördinatie met betrekking tot de afhandeling van deze hack.

Groet, 5.1.2.e

Met vriendelijke groet,

5.1.2.e
DG Digitalisering en Overheidsorganisatie (DGDOO)
.....
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20011 | 2500 EA | Den Haag
.....
T + 5.1.2.e
E 5.1.2.e @minbzk.nl

Van: 5.1.2.e 5.1.2.e @minbzk.nl>
Datum: vrijdag 11 nov. 2022 2:57 PM
Aan: 5.1.2.e ' <5.1.2.e @tweedekamer.nl>, 5.1.2.e <5.1.2.e @tweedekamer.nl>, 5.1.2.e <5.1.2.e @minbzk.nl>, 5.1.2.e ' <5.1.2.e @eerstekamer.nl>, 5.1.2.e <5.1.2.e @minbzk.nl>, 5.1.2.e <5.1.2.e @minbzk.nl>, 5.1.2.e <5.1.2.e @minjenv.nl>
Kopie: Hilvoorde, Marc van <5.1.2.e @minbzk.nl>
Onderwerp: Status ID-ware en uitwerking evaluatiesessie 1 november

Beste mensen,

Bijgaand de uitwerking van de evaluatiesessie van het incident met ID-ware van 1 november. Graag jullie review. 5.1.2.e : 5.1.2.e was aanwezig, maar werkt niet meer bij NCSC, daarom stuur ik hem even naar jou.

De huidige status:

- De onderzoeken bij ID-ware en NCSC zijn afgerond. Hierover is gisteren nog de update in een brief naar de Kamers gestuurd vanuit stass BZK. Dank voor jullie input. In het debat van de stass en MinRb met de Commissie Digitale Zaken van 2 november zijn er geen vragen meer gesteld door de Kamerleden.

- 5.1.2.e heeft een brief van ID-ware ontvangen met excuses, een uitleg en een uitnodiging om details op kantoor van ID-ware te bespreken, mogelijk dat de griffier van de TK een soortgelijke brief heeft ontvangen. Vanuit CIO Rijk gaan we daar gebruik van maken, ik stel voor samen met BVA Rijk. Doel is om zeker te weten dat de juiste maatregelen zijn genomen, die passen bij het belang van de Rijkspas.

- Met NCSC gaan we heldere afspraken op papier zetten voor coördinatie en communicatie bij incidenten en kwetsbaarheden. 5.1.2.e neemt hierbij het voortouw met 5.1.2.e .

- Intern CIO Rijk gaan we de procesgang en assurance rond rijkspas verder verbeteren.

Deze acties worden in de lijn verder opgepakt. Dat betekent dat wat mij betreft na jullie review het responsteam voor de ID-ware hack kan worden opgeheven. Ik hoor graag of jullie het ermee eens zijn.

Groet en fijn weekend,

5.1.2.e

5.1.2.e

.....

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Directie CIO Rijk | DG Overheidsorganisatie
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20011 | 2500 AE | Den Haag

.....

e-mail: 5.1.2.e @minbzk.nl
telefoon secretariaat: 5.1.2.e | mobiel: 5.1.2.e

5.1.2.e

Van: 5.1.2.e <5.1.2.e @minjenv.nl>
Verzonden: donderdag 27 oktober 2022 17:42
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: RE: Evaluatie incident ID-ware

Ik ben volgende week niet beschikbaar in verband met een dienstreis.
Als 5.1.2.e wel kan, dan kan ik vooraf met hem afstemmen vooraf.

Groet,
5.1.2.e

Op 27 okt. 2022 om 12:57 heeft 5.1.2.e <5.1.2.e @minbzk.nl> het volgende geschreven:

Hi allemaal,

Ik heb 5.1.2.e net even telefonisch gesproken omdat eind November zo ver weg is doe ik even een nieuw voorstel.

A.S. dinsdag (1 november) van 13:00 – 14:00
Donderdag 3 november van 12:00 – 13:00 (dan zorgen wij uiteraard dat er een broodje klaar staat voor lunch)

Graag hoor ik zo snel mogelijk of dit uitkomt of dat het mogelijk is dat je iets kan verschuiven, mocht je vragen hebben bel mij gerust!

Met vriendelijke groet,

5.1.2.e

.....
Directie CIO RIJK | Afdeling Directiebureau
Directoraat-generaal Overheidsorganisatie
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Turfmarkt 147 | 2511 DP | Den Haag | 11e etage
Postbus 20011 | 2500 EA | Den Haag
.....
Mobiel: 5.1.2.e
E-mail: 5.1.2.e @minbzk.nl

Algemeen nummer secretariaat: 5.1.2.e
E-mail 5.1.2.e @minbzk.nl

.....
Aanwezig op: maandag, dinsdag, woensdag en donderdag

Bij een bezoek aan het ministerie van BZK is een geldig legitimatiebewijs verplicht!

Van: 5.1.2.e
Verzonden: donderdag 27 oktober 2022 10:24
Aan: 5.1.2.e '5.1.2.e @minjenv.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e

<5.1.2.e @minbzk.nl>; '5.1.2.e @eerstekamer.nl'
<5.1.2.e @eerstekamer.nl>; 5.1.2.e
<5.1.2.e @minjenv.nl>
CC: 5.1.2.e 5.1.2.e @minbzk.nl>
Onderwerp: RE: Evaluatie incident ID-ware

Goedemorgen allen,

Aangezien er op geen van de datums iedereen beschikbaar is zal ik nieuwe datums doorsturen. Dit is dan eind November zodat iedereen hopelijk nog wat ruimte heeft.

Dit gaat om de volgende datums, allen om dezelfde tijd van **13:00 – 14:00.**

Dinsdag 29 november
Woensdag 30 november
Donderdag 1 december

Graag verneem ik of iedereen hiervoor beschikbaar is.

Met vriendelijke groet,

5.1.2.e
.....
Directie CIO RIJK | Afdeling Directiebureau
Directoraat-generaal Overheidsorganisatie
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Turfmarkt 147 | 2511 DP | Den Haag | 11e etage
Postbus 20011 | 2500 EA | Den Haag
.....
Mobiel:
E-mail: 5.1.2.e @minbzk.nl

Algemeen nummer 5.1.2.e
E-mail 5.1.2.e @minbzk.nl

.....
Aanwezig op: maandag, dinsdag, woensdag en donderdag

Bij een bezoek aan het ministerie van BZK is een geldig legitimatiebewijs verplicht!

Van: 5.1.2.e <5.1.2.e @minjenv.nl>
Verzonden: donderdag 27 oktober 2022 09:29
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>;
5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e
<5.1.2.e @minbzk.nl>; '5.1.2.e @eerstekamer.nl'
<5.1.2.e @eerstekamer.nl>; 5.1.2.e
5.1.2.e @minjenv.nl>
CC: 5.1.2.e 5.1.2.e @minbzk.nl>
Onderwerp: RE: Evaluatie incident ID-ware

Allen,

5.1.2.e
Deelname aan de evaluatie zou ik moeten afstemmen met AZ. Het lijkt me geen probleem, maar overleg nog met 5.1.2.e .

Sowieso zal zoveel mogelijk overdragen aan 5.1.2.e of een andere vertegenwoordiger van het NCSC.

5.1.2.e

Van: <5.1.2.e @tweedekamer.nl>
Verzonden: donderdag 27 oktober 2022 08:14
Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e 5.1.2.e @minbzk.nl>; '5.1.2.e @eerstekamer.nl' <5.1.2.e @eerstekamer.nl>; 5.1.2.e 5.1.2.e @minjenv.nl>; 5.1.2.e <5.1.2.e @minjenv.nl>
CC: 5.1.2.e <5.1.2.e @minbzk.nl>
Onderwerp: RE: Evaluatie incident ID-ware

Goedemorgen,

Donderdag 17 november schikt het mij niet, verder kan ik mijn agenda vrij maken voor de andere momenten.

Met vriendelijke groet,

5.1.2.e

Tweede Kamer der Staten-Generaal

Postbus 20018, 2500 EA Den Haag
T +(31)6 21 466 194
E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: woensdag 26 oktober 2022 18:51
Aan: 5.1.2.e ' <5.1.2.e @minbzk.nl>; 5.1.2.e 5.1.2.e @tweedekamer.nl>; 5.1.2.e 5.1.2.e @minbzk.nl>; '5.1.2.e @eerstekamer.nl' 5.1.2.e @eerstekamer.nl>; '5.1.2.e @minjenv.nl' <5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl' 5.1.2.e @minjenv.nl>
CC: 5.1.2.e <5.1.2.e @minbzk.nl>
Onderwerp: RE: Evaluatie incident ID-ware

Beste allen,

Ik kan op alle drie de dagen. Op donderdagochtend ook (als ik wat uit mijn agenda sloop).

Met vriendelijke groet,

5.1.2.e

5.1.2.e

Tweede Kamer der Staten-Generaal
Postbus 20018, 2500 EA Den Haag
T 5.1.2.e | E 5.1.2.e @tweedekamer.nl | I www.tweedekamer.nl

Van: 5.1.2.e <5.1.2.e @minbzk.nl>
Verzonden: woensdag 26 oktober 2022 15:28

Aan: 5.1.2.e <5.1.2.e @tweedekamer.nl>;5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e @eerstekamer.nl' <5.1.2.e @eerstekamer.nl>; 5.1.2.e @minjenv.nl' <5.1.2.e @minjenv.nl>; 5.1.2.e @minjenv.nl' <5.1.2.e @minjenv.nl>
CC: 5.1.2.e <5.1.2.e @minbzk.nl>
Onderwerp: Evaluatie incident ID-ware

Goedemiddag,

Graag plannen wij de afspraak in voor de evaluatie incident ID-ware. Hierbij sturen wij een aantal mogelijkheden door.

Vrijdag 11 november 13:00 – 14:00
Woensdag 16 november 10:00 – 11:00
Donderdag 17 november 10:00 – 11:00

Graag horen wij z.s.m. welke datums er uit komen.

Met vriendelijke groet,

5.1.2.e

.....
Directie CIO RIJK | Afdeling Directiebureau
Directoraat-generaal Overheidsorganisatie
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Turfmarkt 147 | 2511 DP | Den Haag | 11e etage
Postbus 20011 | 2500 EA | Den Haag
.....
Mobiel: 5.1.2.e
E-mail: 5.1.2.e @minbzk.nl

Algemene nummer 5.1.2.e
E-mail secretariaat: 5.1.2.e @minbzk.nl

.....
Aanwezig op: maandag, dinsdag, woensdag en donderdag

Bij een bezoek aan het ministerie van BZK is een geldig legitimatiebewijs verplicht!

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

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Ministry of Justice and Security

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.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

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

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Ministry of Justice and Security

24

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Datum
9 november 2022

Kenmerk

verslag evaluatie ID-ware (concept)

Vergaderdatum	1 november 2022
Aanwezig	CISO-Rijk (vz), vertegenwoordiging van betrokken organisaties: Tweede Kamer, Eerste Kamer, NCSC, CIO-Rijk/IB&P, Rijks-BVA.
Afwezig	CIO-Rijk/programmamanagement Rijkspas.

Op 1 november 2022 evalueerden bovengenoemde betrokkenen het incident: wat ging goed en wat kan beter. Wat zijn de te nemen acties.
Dit document verslag is geen woordelijk verslag van hetgeen is gezegd, maar geeft de belangrijkste noties, bevindingen en aanbevelingen tot vervolg weer op 4 onderdelen: 'incident'; 'coördinatie'; 'communicatie', 'verder onderzoeken en verbeterpunten'. In definitieve vorm is de feedback van de aanwezigen verwerkt.

1. Incident

Wat is er gebeurd (er is een gedetailleerde tijdlijn gemaakt, hieronder een globale schets):

- 21 sept: 5.1.2.e TK belt 5.1.2.e Rijk met nog niet heel duidelijke boodschap vanuit de leverancier- focus lag op bedrijfscontinuiteit. Meer informatie na het weekend.
- 28 sept: TK/EK en TBRV (beheer Rijkspasvoorziening) ontvangen bericht van ID-ware over dat zij getroffen zijn door een ransomware aanval en dat hierbij bestanden zijn geëxfiltreert.
- Beheerorganisatie Rijkspas (P-direkt organisatie) informeert 5.1.2.e Rijk en later nogmaals toen de ernst zichtbaarder werd. 5.1.2.e Rijk heeft toen ook 5.1.2.e-Rijk gebeld
- Melding datalek bij AP door Rijkspas beheer, Tweede/Eerste Kamer (TK/EK) TK/EK en ID-ware.
- 30 sept: afspraak samenwerking TK/EK en 5.1.2.e en 5.1.2.e Rijk; eerste overleg met NCSC.
- 2 okt: Formeel ondersteuningsverzoek van 5.1.2.e Rijk aan NCSC. Communicatiescenario's opgesteld.
- 3 okt: breed overleg vanuit NCSC met ID-ware, politie, AIVD, NCTV, TK, EK, 5.1.2.e-Rijk

- NCTV organiseert twee bestuurlijke overleggen gericht op de risico's voor DKDB en mogelijke escalatie in de crisisstructuur.
- 7 okt: informeren van pasgebruikers en brief van stass BZK aan TK en EK, media-aandacht

Wat losse noties:

- 5.1.2.f [redacted] Logging laat zien dat een grote heoeveelheid data is geëxfiltreerd. De lijst met 75.000 bestanden is via een leak-site verkregen.
- 5.1.2.f [redacted]

Openstaande- en verbeterpunten:

- Risicoduiding van de gelekte identiteitsgegevens met name paspoort foto's.
  Advies, actie: raadpleeg de collega's van RvIG over de mogelijke nadelige gevolgen ervan voor de betrokkenen (TK/EK)
- Er zaten oude gegevens 2013 in de set –
  Advies, actie: opnemen in verder te onderzoeken - hoe zit het met de vernietigingstermijnen (afgesproken en gerealiseerde termijnen) .

2. Coördinatie

Wat ging goed

- Een app groep (signal) voor overleg en communicatie
- Woordvoering betrekken t.b.v. communicatie

Wat ging niet goed, verbeterpunten

- In eerste instantie onduidelijkheid wie hier in de lead zou moeten zijn (2 verschillende soorten dienstverlening met verschillende contracten), dit is pragmatisch opgelost.
- Omvang opschaling wordt snel groot door groot aantal betrokken partijen
- 5.1.2.h [redacted]
- Ook de dienst had eerder betrokken willen zijn ivm de aard van de aanval.
- Voor de betrokkenheid van het NCSC is duidelijkheid nodig of dit primair een cyberincident is of primair een datalek voor de inzet. Achteraf was met name het datalek een probleem.
- De BOB-methode werd vanaf het begin toegepast, wat hielp om het beeld aan te scherpen en vervolgacties te bepalen
- **Afspraak:** BZK en NCSC maken in de koude fase afspraken over coördinatie en communicatie bij incidentescalatie.

- **Afspraak:** Afspraak met ID-ware maken om de maatregelen te beoordelen

3. Communicatie

Wat ging goed

- Omvang van de boodschap is goed afgestemd
- Stass BZK kon de pers na de MR goed te woord staan, was goed en tijdig geïnformeerd
- Brief 7 oktober was goed gevallen, zorgde voor de-escalatie in de pers.
- "Stick tot the plan": de communicatiescenario's die al vroeg zijn opgesteld, met hierin triggers voor communicatie, heeft geholpen om keuzes te maken en uiteindelijk op het juiste moment en de juiste volgorde te communiceren.

Wat ging niet goed, verbeterpunten

- Niet altijd duidelijk wat je wel of niet kunt delen - Persoonsgegevens altijd minimaal delen.
- Communicatie verliep rommelig – info via meer kanalen, TBRV communiceerde te vroeg, uiteindelijk is de goede volgorde aangehouden: eerst intern communiceren, daarna de brief van stass naar TK/EK. Dit volgde elkaar snel op.
- Vanuit eigenaarschap Rijkspas niet aangesloten en niet aanwezig
- CISO's en BVA's eerder d.m.v. heads-up informeren, zodat duidelijk is dat de respons gecoördineerd wordt. Informeren was nu een dag voordat breder gecommuniceerd werd met een mailbericht over het incident en de status. Privacy Officers gelijk meenemen met CISO's en BVA's.
- Dienst was geïnformeerd, maar ervaarde te laat erbij betrokken te zijn (3okt) zie ook bij coördinatie.
- Er waren tegenstrijdige berichten (wel niet 2de Kamerleden)

4. Verder onderzoeken en verbeterpunten

Verbeterpunten benoemd

- Meteen via de eigenaars van systeem -coördinatie tav TVRB

Verbeterpunten uit 1,2 en 3 (adviezen en afspraken)

- **Advies, actie**: raadpleeg de collega's van RvIG over de mogelijke nadelige gevolgen van het lekken van paspoortgegevens m.n. pasfoto's voor de betrokkenen (actie TK/EK?)
- **Advies, actie**: opnemen in verder te onderzoeken - hoe zit het met de vernietigingstermijnen bij ID-ware (afgesproken en gerealiseerde termijnen) (actie CIO Rijk)
- **Afspraak:** BZK en NCSC maken in de koude fase afspraken over coördinatie en communicatie bij incidentescalatie (actie CISO-Rijk).

Nog nader te onderzoeken (CISO-Rijk)

- Zijn de door ID-ware doorgevoerde maatregelen adequaat tav dit incident.
- Wat is de staat van beveiliging bij Rijkspas dienstverleners (scope Rijksbrede voorziening)
- 5.1.2.b
- Vernietigingstermijnen (zie verbeter punt 2 hierboven)

25

5.1.2.e

Van: 5.1.2.e <5.1.2.e @minjenv.nl>
Verzonden: woensdag 2 november 2022 13:25
Aan: 5.1.2.e
CC: 5.1.2.e
Onderwerp: FW: Vragen FD over hack ID-Ware

Hoi 5.1.2.e,

Zoals afgesproken bijgaand de tekst die wij bij woordvoering hebben aangeleverd in antwoord op de vragen van FD.

Gr 5.1.2.e

Van: 5.1.2.e
Verzonden: vrijdag 28 oktober 2022 14:12
Aan: 5.1.2.e <5.1.2.e @minjenv.nl>
CC: 5.1.2.e <5.1.2.e @ncsc.nl>; 5.1.2.e <5.1.2.e @minjenv.nl>
Onderwerp: FW: Vragen FD over hack ID-Ware

Hoi 5.1.2.e,

Zie onderstaand de intern NCSC afgestemde beantwoording. Stem jij verder af met evt. NCTV/BZK?

Gr 5.1.2.e

Van: 5.1.2.e <5.1.2.e @minjenv.nl>
Verzonden: vrijdag 28 oktober 2022 14:07
Aan: 5.1.2.e <5.1.2.e @minjenv.nl>
Onderwerp: RE: Vragen FD over hack ID-Ware

Heel heldere weergave, Collin. Helemaal akkoord dus zo.

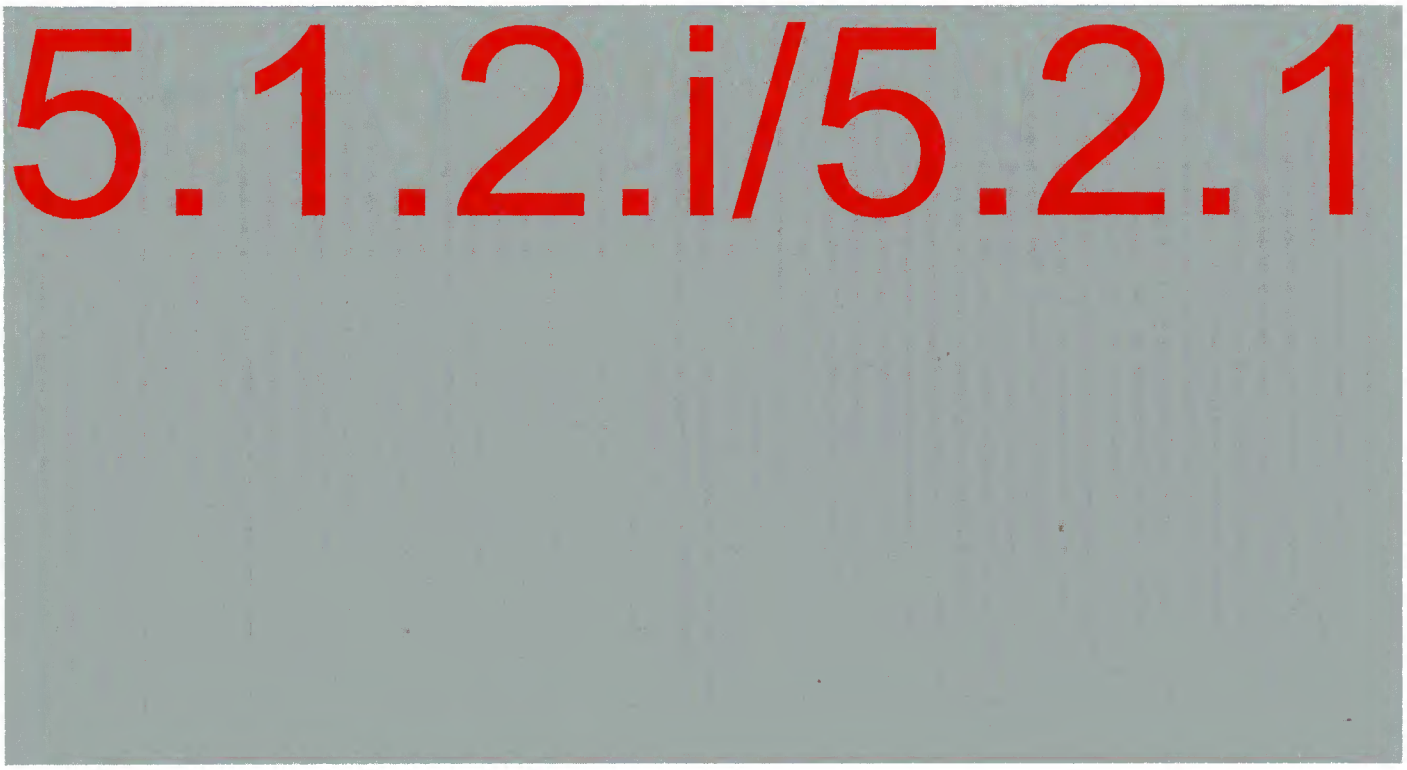
Grtz,
5.1.2.e

Verzonden met BlackBerry Work
(www.blackberry.com)

Van: 5.1.2.e <5.1.2.e @minjenv.nl>
Datum: vrijdag 28 okt. 2022 1:49 PM
Aan: 5.1.2.e <5.1.2.e @minjenv.nl>
Kopie: 5.1.2.e <5.1.2.e @minjenv.nl>, 5.1.2.e <5.1.2.e minjenv.nl>, 5.1.2.e <5.1.2.e >, 5.1.2.e <5.1.2.e @ncsc.nl>, 5.1.2.e <5.1.2.e @minjenv.nl>
Onderwerp: FW: Vragen FD over hack ID-Ware

Hoi 5.1.2.e,

Zie hieronder de met 5.1.2.e 5.1.2.e 5.1.2.e en 5.1.2.e afgestemde conceptbeantwoording. Ik heb de "schone" versie hieronder geknipt en geplakt.



Graag je akkoord voor verzending aan 5.1.2.e.

Gr 5.1.2.e

Van: 5.1.2.e <5.1.2.e @minjenv.nl>
Verzonden: vrijdag 28 oktober 2022 11:28
Aan: 5.1.2.e <5.1.2.e @minjenv.nl>
Onderwerp: FW: Vragen FD over hack ID-Ware

Hi 5.1.2.e,

Hierbij de vragen. Laten we inderdaad ook even bellen.

Groet,
5.1.2.e

Met vriendelijke groet,

5.1.2.e

.....
Ministerie van Justitie en Veiligheid
Directie Communicatie
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
.....
M 5.1.2.e
5.1.2.e @minjenv.nl
www.rijksoverheid.nl/jenv

.....

Voor een rechtvaardige en veilige samenleving

.....

Van: 5.1.2.e <5.1.2.e @fd.nl>
Verzonden: vrijdag 28 oktober 2022 11:00
Aan: 5.1.2.e <5.1.2.e @minjenv.nl>
Onderwerp: Vragen FD over hack ID-Ware

Hoi 5.1.2.e,

Hierbij mijn vragen over de hack bij ID-ware. Vandaag komt ID-Ware met een statement over het afronden van het onderzoek naar de hack. Mij is inmiddels duidelijk dat de omvang van de hack vele malen groter is dan in eerste instantie werd gecommuniceerd.

- Welke rol heeft de NCSC nou precies gespeeld in de nasleep van deze hack? Getroffen klanten (niet-overheid) vertellen mij dat de NCSC hen informeert over de stand van zaken en het aantal gelekte persoonsgegevens?
- Van hoeveel personen zijn de persoonsgegevens precies buitgemaakt?

Groet!

5.1.2.e

Prins Bernhardplein 173, 1097 BL Amsterdam
Postbus 216, 1000 AE Amsterdam
5.1.2.e
5.1.2.e @fd.nl
www.fd.nl
Onderdeel van FD Mediagroep

IDware

ID-ware International B.V. | Mesdagstraat 118 | 2596 XZ Den Haag

CIO-Rijk
t.a.v. 5.1.2.e
Postbus 20011
2500 EA DEN HAAG

The Netherlands

Den Haag, 4 november 2022

Referentie: 5.1.2.e

Geachte heer Lourens Visser,

Bijgaand vindt u een brief aangehangen betreffende de ransomware-aanval ID-ware.

5.1.2.e

5.1.2.e

IDware

CIO-Rijk
t.a.v. 5 1 2.e
Postbus 20011
2500 EA DEN HAAG

Den Haag, 4 november 2022

Betreft: Ransomware-aanval ID-ware

Geachte 5 1 2 e

Hierbij benader ik u in verband met de ransomware-aanval van 17 september op de systemen van ID-ware, waarbij onder meer data van de Rijksoverheid is gelekt.

Allereerst wil ik u namens ID-ware mijn welgemeende excuses aanbieden voor de negatieve gevolgen die de Rijksoverheid en uw directie van deze aanval ondervindt. De aanval en het sensitieve karakter van de gelekte persoonlijke data hebben vanzelfsprekend tot zorgen geleid bij de gebruikers van de diensten die wij aan de Rijksoverheid bieden en tot twijfels over de veiligheid van onze infrastructuur. Ik betreur ten zeerste dat de onze klanten getroffen zijn door deze criminele daad. Ik garandeer u dat wij ons maximaal blijven inzetten om onze cyberweerbaarheid te verhogen teneinde herhaling te voorkomen.

Alvorens de onderzoeksbevindingen aan u toe te lichten, wil ik graag nog mijn dank uitspreken voor de nauwe samenwerking met medewerkers van uw organisatie in deze voor iedereen vervelende en hectische periode.

Onlangs hebben wij het onderzoek afgerond naar de volledige omvang van de aanval. In het tweede gedeelte van deze brief geef ik u graag nadere context en uitleg over de ransomware-aanval, de gevolgde procedures, de uitkomsten van de analyses binnen de getroffen Rijksoverheid-organisaties en de door ons genomen maatregelen om herhaling te voorkomen.

De ransomware-aanval

Op zondag 18 september hebben wij vastgesteld dat een deel van onze IT-servers niet meer beschikbaar was. Wij bleken slachtoffer te zijn geworden van een ransomware-aanval. Daarop hebben wij direct actie ondernomen en gehandeld in lijn met de geldende wet- en regelgeving: binnen 24 uur zijn gerenommeerde externe cybersecurity experts van Fox-IT aan de slag gegaan, die een onderzoek hebben uitgevoerd naar de aard van de aanval en de betrokken gegevens. De operatie kon met behulp van adviezen van Fox-IT snel en met aangescherpte veiligheid hersteld worden.

De aanval is uitgevoerd door de bekende ransomware-groep "BlackCat" alias "ALPHV". ID-ware heeft een verzoek tot losgeld gekregen waar wij, conform richtlijnen van onder andere de High Tech Crime Unit van de Politie, geen gehoor aan hebben gegeven. Er is melding gedaan bij de Autoriteit Persoonsgegevens en wij zijn sindsdien in voortdurend contact geweest met de Politie, waar tevens aangifte gedaan is, de Rijksoverheid en het Nationaal Cyber Security Centrum.

Onderzoeksbevindingen Fox-IT en ID-ware

Wij hebben in samenwerking met cybersecurity experts van Fox-IT een analyse uitgevoerd om de totale omvang en consequenties van de ransomware-aanval vast te stellen. Fox-IT heeft een rapport opgesteld van het onderzoek dat zij heeft uitgevoerd naar de oorzaak en omvang van het incident en heeft ons geadviseerd over de te nemen maatregelen. In bijlage I bij deze brief vindt u de management samenvatting van het onderzoeksrapport van Fox-IT. Ik wil u graag de mogelijkheid aanbieden om het volledige rapport bij ons op kantoor in te zien.

Door Fox-IT is vastgesteld dat de ransomware-groep vanuit de ID-ware infrastructuur data geëxfiltreerd en gepubliceerd heeft op het Dark Web. Fox-IT heeft ons een lijst aangereikt met daarin de bestandsnamen van de gepubliceerde data. Deze bestandsnamen zijn bevestigd en ook aan ons verstrekt door het NCSC. De getroffen bestanden zijn door ons in de afgelopen weken geanalyseerd. Klanten van onze diensten waarvan is vastgesteld dat er gegevens zijn gelekt, zijn daarvan direct op de hoogte gesteld en doorlopend geïnformeerd zodra nieuwe informatie werd gedetecteerd.

Voor wat betreft de Rijkspasvoorziening, waarvoor ID-ware beheerdiensten en gebruikersondersteuning levert, hebben we vrijwel dagelijks contact met 5 1 2 e

De Rijkspassystemen zelf worden gehost binnen de infrastructuur van het Rijk, die geen onderdeel was van de aanval. Wel betreuren we het dat uit het onderzoek is gebleken dat van 3200 Belastingdienst-medewerkers het thuisbezorgbewijs is gelekt, met daarin hun naam, digitale paraaf en het Rijkspasnummer.

5 1 2 h

5.1.2.h Wij hebben de lijst met getroffen afleverbewijzen gedeeld met de Belastingdienst en samen met het Rijkspasteam van uw organisatie ondersteuning geboden waar nodig of gewenst.

Voor wat betreft de gelekte data van de Eerste en Tweede Kamer populatie onderhouden we onder meer contacten met de 5.1.2.e r. ID-ware levert een SAAS-oplossing voor cardmanagement rechtstreeks aan de Tweede Kamer. Deze oplossing draait op ID-ware omgevingen die getroffen zijn door de aanval. Er worden geen Rijkspassen door ID-ware geproduceerd en ook het sleutelmateriaal op de passen is niet in bezit van ID-ware. Het systeem is in goed overleg met de Tweede Kamer inmiddels weer in productie genomen.

Tot slot ga ik ervan uit dat u op de hoogte bent dat ook de 5.1.2.f helaas getroffen zijn door de aanval op onze systemen. ID-ware levert aan 5.1.2.f dit betreft geen Rijkspassen. Deze oplossing draait op ID-ware omgevingen die wel onderdeel van de aanval waren. Ook met die partijen onderhouden we uiteraard nauwe contacten over de gevolgen.

Maatregelen om herhaling te voorkomen

Op advies van Fox-IT hebben wij meteen al een aantal aanvullende veiligheidsmaatregelen getroffen om de systemen te herstellen, potentieel restrisico te limiteren en om de bron van het incident te identificeren om zo herhaling in de toekomst te voorkomen. Deze maatregelen omvatten onder meer 5.1.2.f

. Een overzicht van algemene en specifieke maatregelen in de context van de Rijksoverheid vindt u in de bijlage II bij deze brief.

Graag willen wij het bovenstaande in een persoonlijk gesprek nader toelichten, zodat u meer inzicht kan krijgen in de aard en consequenties van de ransomware-aanval en de door ons getroffen maatregelen. Mocht u het volledige rapport van 5.1.2.f in willen zien, dan maken wij dat ook graag mogelijk op locatie bij ID-ware.

Vanzelfsprekend ben ik beschikbaar voor vragen of nadere informatie.

Hoogachtend,

5.1.2.e

5.1.2.e

IDware

Bijlage I: Management samenvatting – rapport 5.1.2 f (aanvalsanalyse)

- 5.1.2 h [redacted]
- 5.1.2 f heeft vastgesteld dat met 5.1.2 h [redacted] kwaadaardige activiteiten uitgevoerd zijn en in de nacht van 17 september de aanvaller data naar een extern systeem heeft overgebracht.
- Onze bestaande veiligheidscontroles hebben de kwaadaardige activiteit onvoldoende gedetecteerd of vertraagd, waardoor de ransomware-aanval kon slagen en data onttrokken kon worden 5.1.2 h [redacted]

5.1.2.h

- 5.1.2 f acht het waarschijnlijk dat de data en omvang had van 221 GB aan gegevens. Kort hierna werd malware, geïdentificeerd als BlackCat ransomware, uitgevoerd op systemen binnen het ID-ware domein.
- Specifieke data die door de aanval verzameld is, is op een darknet-website gepubliceerd. De website stelt dat 73.358 bestanden beschikbaar zijn, met een totale omvang van 27,6 GB. 5.1.2 f heeft dit bevestigd. Een klein deel van deze bestanden bevat helaas data van personen die aan de Rijksoverheid verbonden zijn.
- 5.1.2 f heeft sporen gevonden van bestandsversleuteling door de ransomware 5.1.2 h [redacted] in de omgeving van ID-ware.

IDware

Bijlage II: Genomen maatregelen door ID-ware na de ransomware-aanval

Algemeen

- 5.1.2.h [redacted]

Rijksoverheid

- 5.1.2.h [redacted]

Deutsche Post
FI 18.11.22 7,20

F1 011C 0814
00 28D4 6382

Recommandé

R

RT 12 512 586 5DE

Ontvangen

27

5.1.2.e

Van: 5.1.2.e
Verzonden: donderdag 24 november 2022 09:19
Aan: 5.1.2.e
Onderwerp: archivering digidoc FW: Status ID-ware en uitwerking evaluatiesessie 1 november
Bijlagen: Buiten reikwijdte

Goedemorgen 5.1.2.e

Er zijn op de evaluatie van ID-ware door betrokkenen een paar reacties binnengekomen.

5.1.2.e : dank en bevestiging van de juiste aanpak
5.1.2.e : oneens met onderstaande en niet akkoord zonder correcties – inhoudelijke correcties zijn verder niet aangedragen – gesprek hierover ligt op managementniveau; Het is altijd nog mogelijk om later een erratum of addendum op dit verslag toe te voegen indien nodig.
Van anderen geen reactie ontvangen

We bespraken dat dit dan ook vooralsnog de definitieve versie is.
Ik zal deze mail en bijlage voor je opslaan in digidoc, zoals eerder afgesproken.

met vriendelijke groet,

5.1.2.e

Van: 5.1.2.e <5.1.2.e @minbzk.nl>
Verzonden: vrijdag 11 november 2022 14:58
Aan: 5.1.2.e ' <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e ' <5.1.2.e @eerstekamer.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @minjenv.nl>
CC: 5.1.2.e <5.1.2.e @minbzk.nl>
Onderwerp: Status ID-ware en uitwerking evaluatiesessie 1 november

Beste mensen,

Bijgaand de uitwerking van de evaluatiesessie van het incident met ID-ware van 1 november. Graag jullie review.
@5.1.2.e : 5.1.2.e was aanwezig, maar werkt niet meer bij NCSC, daarom stuur ik hem even naar jou.

De huidige status:

- De onderzoeken bij ID-ware en NCSC zijn afgerond. Hierover is gisteren nog de update in een brief naar de Kamers gestuurd vanuit stass BZK. Dank voor jullie input. In het debat van de stass en MinRb met de Commissie Digitale Zaken van 2 november zijn er geen vragen meer gesteld door de Kamerleden.

- 5.1.2.e heeft een brief van ID-ware ontvangen met excuses, een uitleg en een uitnodiging om details op kantoor van ID-ware te bespreken, mogelijk dat de griffier van de TK een soortgelijke brief heeft ontvangen. Vanuit CIO Rijk gaan we daar gebruik van maken, ik stel voor samen met 5.1.2.e. Doel is om zeker te weten dat de juiste maatregelen zijn genomen, die passen bij het belang van de Rijkspas.

- Met NCSC gaan we heldere afspraken op papier zetten voor coördinatie en communicatie bij incidenten en kwetsbaarheden. 5.1.2.e neemt hierbij het voortouw met 5.1.2.e .

- Intern CIO Rijk gaan we de procesgang en assurance rond rijkspas verder verbeteren.

Deze acties worden in de lijn verder opgepakt. Dat betekent dat wat mij betreft na jullie review het responsteam voor de ID-ware hack kan worden opgeheven. Ik hoor graag of jullie het ermee eens zijn.

Groet en fijn weekend,

5.1.2.e

5.1.2.e

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Directie CIO Rijk | DG Overheidsorganisatie
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20011 | 2500 AE | Den Haag

e-mail: 5.1.2.e @minbzk.nl
telefoon secretariaat: 5.1.2.e | mobiel: 5.1.2.e

28

5.1.2.e

Van: 5.1.2.e
Verzonden: maandag 31 oktober 2022 08:25
Aan: 5.1.2.e
Onderwerp: RE: Via e-mail verzenden: 02. Kamerbrief hack bij ID-ware.docx
Bijlagen: Buiten reikwijdte

Ha 5.1.2.e collega,
Ik heb de reviews van Jaqueline en Rik samengevoegd en nog een paar typo's aanvullend gecorrigeerd, zie bijlage

met vriendelijke groet,

5.1.2.e

-----Oorspronkelijk bericht-----
Van: 5.1.2.e <5.1.2.e @tweedekamer.nl>
Verzonden: vrijdag 28 oktober 2022 18:30
Aan: 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <m5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>
Onderwerp: RE: Via e-mail verzenden: 02. Kamerbrief hack bij ID-ware.docx

Beste 5.1.2.e

Bij dezen.

Met vriendelijke groet,
5.1.2.e
Hoofd Bureau CISO Tweede Kamer der Staten-Generaal Postbus 20018, 2500 EA Den Haag T 06 1830 5705 | E H.Driessen@tweedekamer.nl | I www.tweedekamer.nl

-----Oorspronkelijk bericht-----
Van: 5.1.2.e <5.1.2.e @minbzk.nl>
Verzonden: vrijdag 28 oktober 2022 16:46
Aan: 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @tweedekamer.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>; 5.1.2.e <5.1.2.e @minbzk.nl>
Onderwerp: Via e-mail verzenden: 02. Kamerbrief hack bij ID-ware.docx

En de brief aan de kamer, in concept. Graag jullie opmerkingen.

Groet,

5.1.2.e

Uw bericht kan nu met de volgende bijlagen of koppelingen worden verzonden:

02. Kamerbrief hack bij ID-ware.docx


vodafone NL
22:07
Coördinatie ID-Ware
Coördinatie ID-Ware
7 leden
za 1 okt.
Je hebt de groep aangemaakt.
Je kunt vrienden en kennissen voor deze groep uitnodigen via een groepslink
Kennissen uitnodigen
8
Groep aangemaakt om s
overleg te kunnen plannen
Nieuw bericht

vodafone NL 22:08

Coördinatie ID-Ware

Groep aangemaakt om snel overleg te kunnen plannen

za 1 okt.

Voorstel is om rond 16:00 telefonisch te overleggen.

13:36

5.1.2.e

5.1.2.e

Oke! 13:38

5.1.2.e

5.1.2.e 13:41

5.1.2.e

5.1.2.e

Ok graag via beeld 13:49

5.1.2.e

Dat lukt voor mij niet...

5.1.2.e

telefoon.call 13:53

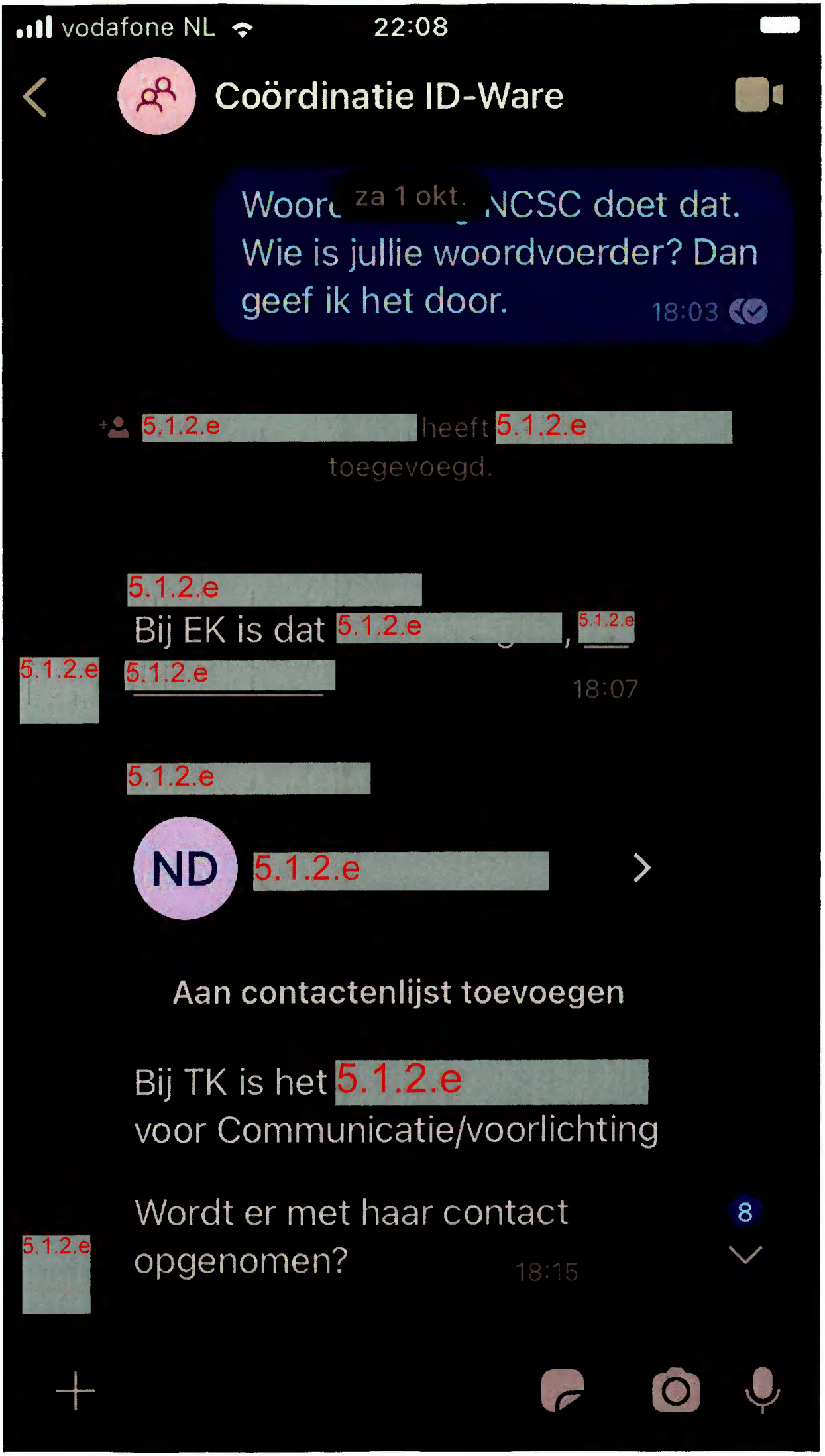
8

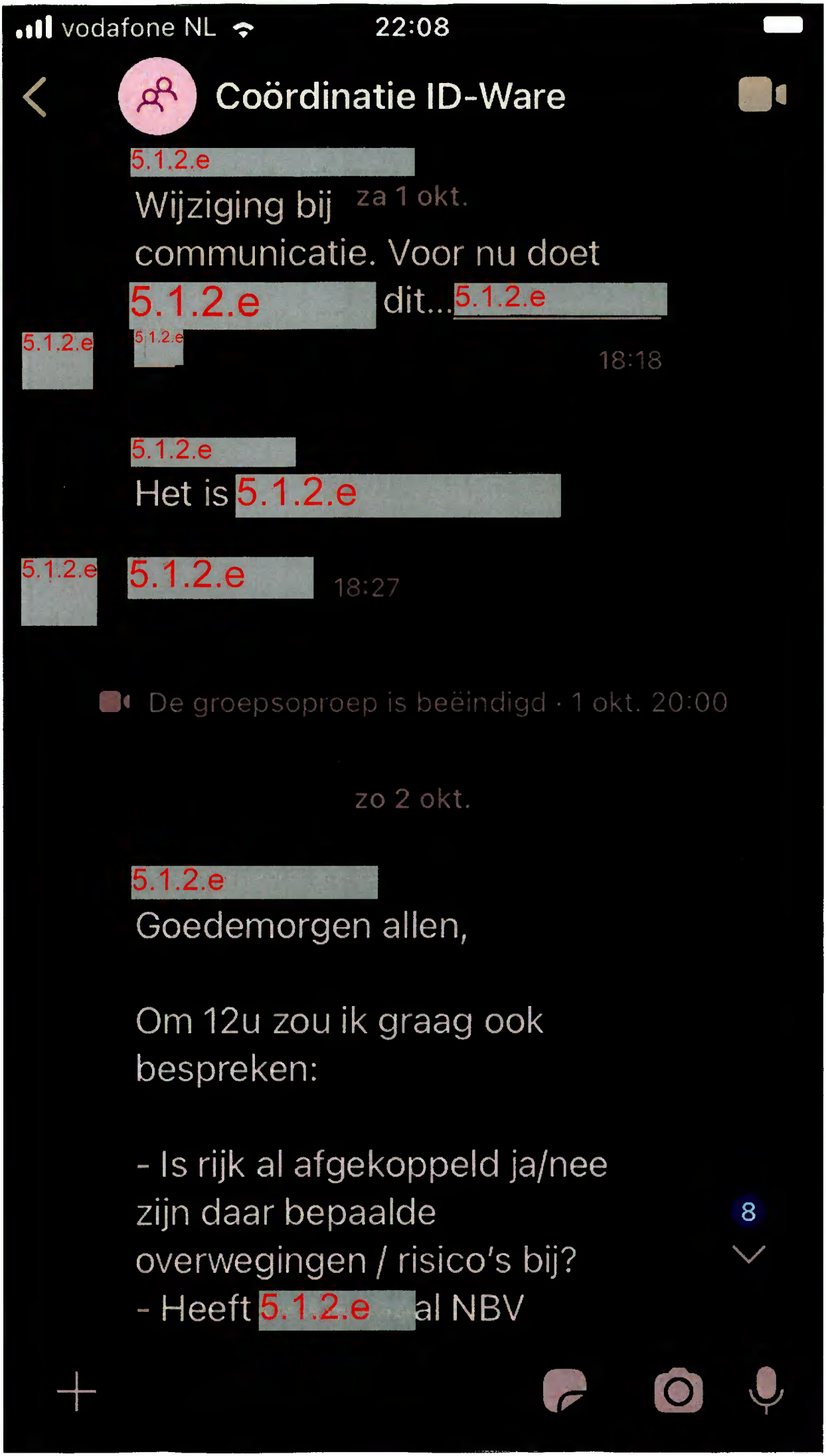
5.1.2.e

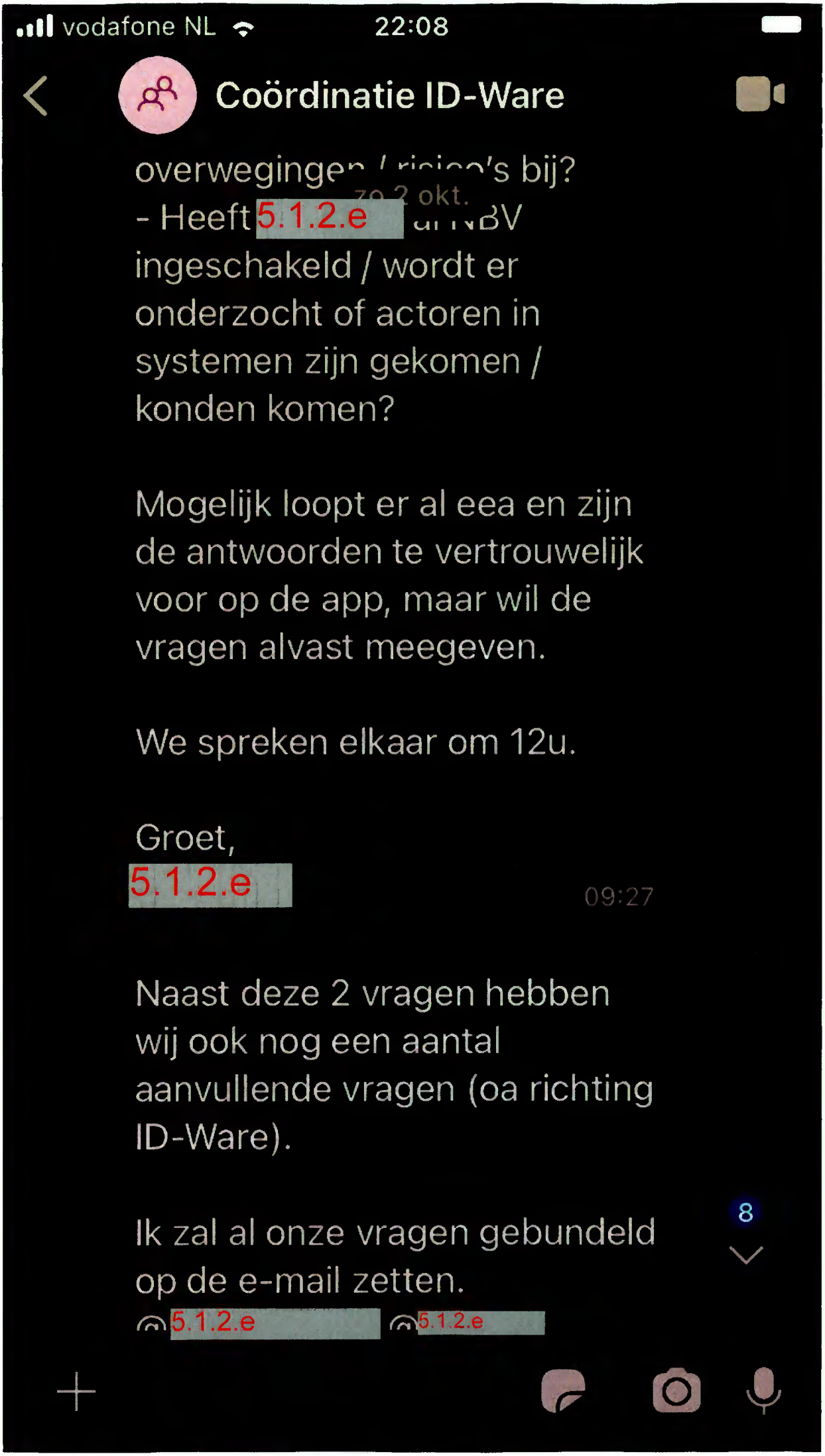
5.1.2.e

Ok 13:54


vodafone NL
22:08
Coördinatie ID-Ware
5.1.2.e
Ok 13:54
za 1 okt.
Ik ga een compromis proberen: beeld via Signal... 14:37
5.1.2.e
Ik ben waarschijnlijk onderweg dus vandaar..hebben toch geen beeld nodig...ja, van het incident 14:39
De groepsoproep is beëindigd · 1 okt. 16:00
5.1.2.e
@5.1.2.e heb jij al een persoon die regie voert op communicatie en waar onze woordvoerder/communicatie mee kan schakelen? 18:02
8
Woordvoering NCSC doet da
Wie is jullie woordvoerder? Dan


vodafone NL
22:08
Coördinatie ID-Ware
za 1 okt.
Woor NCSC doet dat. Wie is jullie woordvoerder? Dan geef ik het door.
18:03
5.1.2.e heeft 5.1.2.e toegevoegd.
5.1.2.e
Bij EK is dat 5.1.2.e , 5.1.2.e
5.1.2.e 5.1.2.e
18:07
5.1.2.e
ND
5.1.2.e
Aan contactenlijst toevoegen
Bij TK is het 5.1.2.e voor Communicatie/voorlichting
Wordt er met haar contact opgenomen?
5.1.2.e
18:15
8


vodafone NL
22:08
Coördinatie ID-Ware
5.1.2.e
Wijziging bij communicatie. Voor nu doet 5.1.2.e dit...5.1.2.e
za 1 okt.
5.1.2.e
5.1.2.e
18:18
5.1.2.e
Het is 5.1.2.e
5.1.2.e
5.1.2.e
18:27
De groepsoproep is beëindigd · 1 okt. 20:00
zo 2 okt.
5.1.2.e
Goedemorgen allen,
Om 12u zou ik graag ook bespreken:
- Is rijk al afgekoppeld ja/nee zijn daar bepaalde overwegingen / risico's bij?
- Heeft 5.1.2.e al NBV
8


vodafone NL
22:08
Coördinatie ID-Ware
overwegingen / risico's bij?
- Heeft 5.1.2.e
ingeschakeld / wordt er
onderzocht of actoren in
systemen zijn gekomen /
konden komen?
Mogelijk loopt er al eea en zijn
de antwoorden te vertrouwelijk
voor op de app, maar wil de
vragen alvast meegeven.
We spreken elkaar om 12u.
Groet,
5.1.2.e
09:27
Naast deze 2 vragen hebben
wij ook nog een aantal
aanvullende vragen (oa richting
ID-Ware).
Ik zal al onze vragen gebundeld
op de e-mail zetten.
5.1.2.e
5.1.2.e

vodafone NL 22:08

Coördinatie ID-Ware

zo 2 okt.

Naast deze 2 vragen hebben wij ook nog een aantal aanvullende vragen (oa richting ID-Ware).

Ik zal al onze vragen gebundeld op de e-mail zetten.
@5.1.2.e @5.1.2.e
5.1.2.e ik heb jullie e-mailadressen alleen nog niet: zou ik die mogen? 10:33

5.1.2.e

5.1.2.e

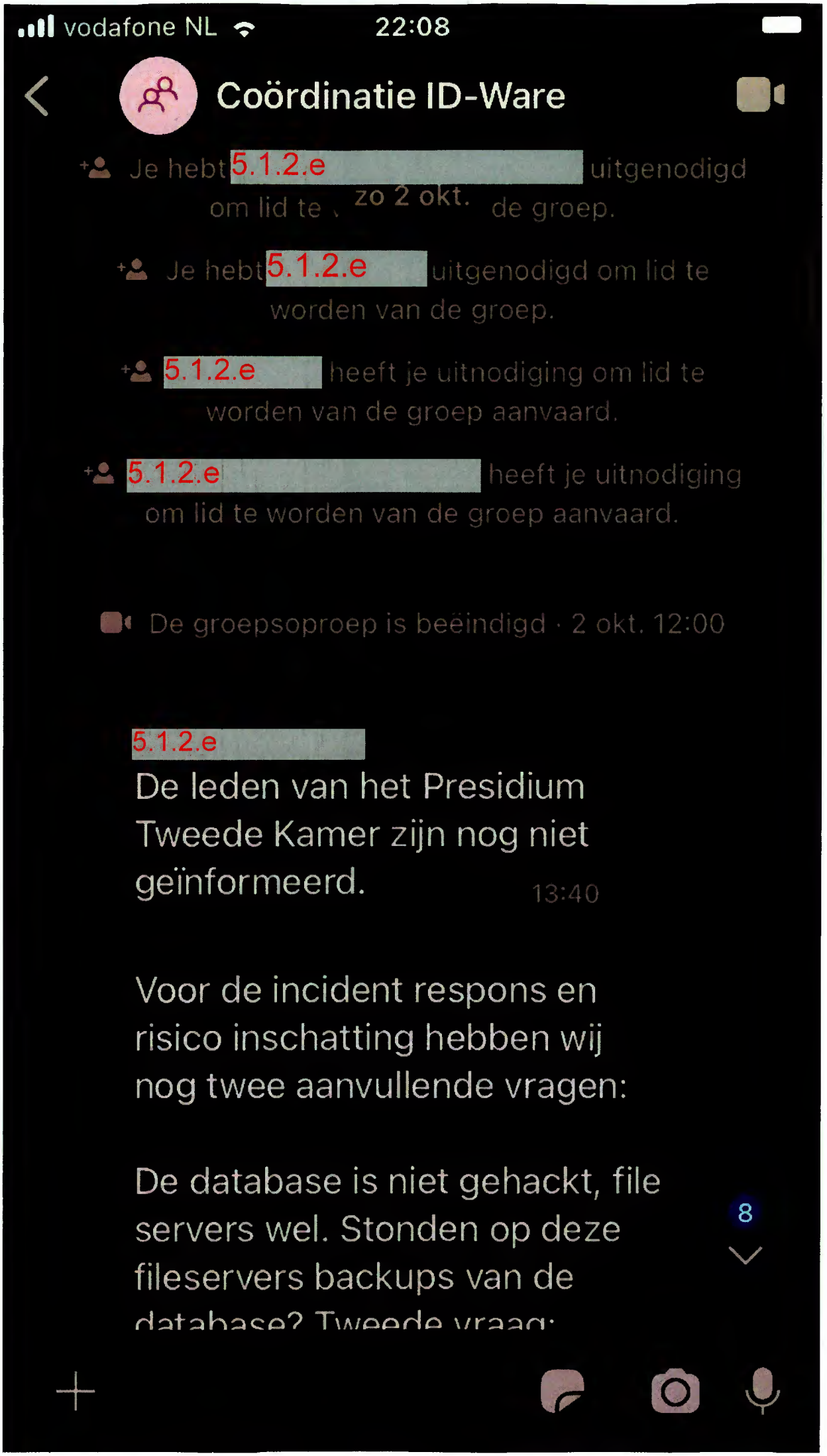
5.1.2.e 5.1.2.e 10:34

5.1.2.e

Heb mailadres 5.1.2.e met 5.1.2.e gedeeld 10:36

Je hebt 5.1.2.e uitgenodigd om lid te worden van de groep. 8

Je hebt 5.1.2.e uitgenodigd om lid te


vodafone NL
22:08
Coördinatie ID-Ware
Je hebt 5.1.2.e uitgenodigd om lid te zo 2 okt. de groep.
Je hebt 5.1.2.e uitgenodigd om lid te worden van de groep.
5.1.2.e heeft je uitnodiging om lid te worden van de groep aanvaard.
5.1.2.e heeft je uitnodiging om lid te worden van de groep aanvaard.
De groepsoproep is beëindigd · 2 okt. 12:00
5.1.2.e
De leden van het Presidium Tweede Kamer zijn nog niet geïnformeerd.
13:40
Voor de incident respons en risico inschatting hebben wij nog twee aanvullende vragen:
De database is niet gehackt, file servers wel. Stonden op deze fileservers backups van de database? Tweede vraag:
8

vodafone NL 22:08

Coördinatie ID-Ware

Voor de inci zo 2 okt. ons en risico inschatting hebben wij nog twee aanvullende vragen:

De database is niet gehackt, file servers wel. Stonden op deze fileservers backups van de database? Tweede vraag; draaiden de databases op en databaseserver of als dbms geïmplementeerd op een fileserver?

Zouden deze vragen met prio meegenomen kunnen worden namens ons? 13:47

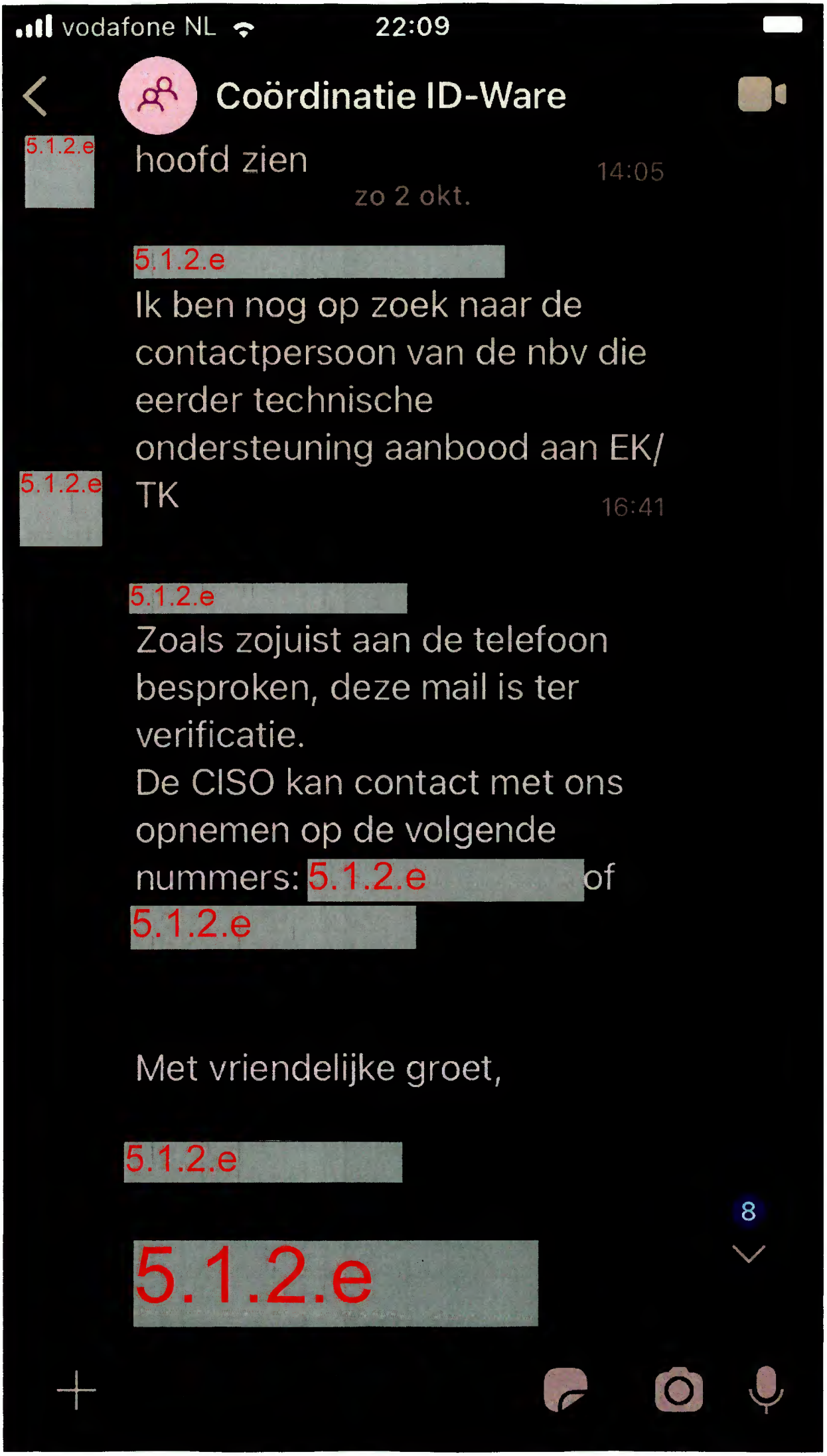
5.1.2.e

5.1.2.e

Net weer THTC gesproken, ze hebben net als 5.1.2.f nog geen back-ups in de 75.000 geexfiltreerde bestanden gespot.. maar ze hebben nog maar een dag de tijd gehad dus

8


vodafone NL
22:08
Coördinatie ID-Ware
5.1.2.e
zo 2 okt.
Net weer THTC gesproken, ze hebben net als 5.1.2.f nog geen back-ups in de 75.000 geexfiltreerde bestanden gespot.. maar ze hebben nog maar een dag de tijd gehad dus vandaar de slag om de arm
13:57
uit openbare technische documentatie van een universiteit klant leid ik af dat in ieder geval van sommige klanten in het verleden een volledige DBMS server gebruikt is en als de "boefjes" zoals de politie ze noemt snel klaar willen zijn is het denkbaar dat ze zo een "hoofdprijs" over het hoofd zien
5.1.2.e
14:05
8
5.1.2.e
Ik ben nog op zoek naar de


vodafone NL
22:09
Coördinatie ID-Ware
5.1.2.e
hoofd zien
14:05
zo 2 okt.
5.1.2.e
Ik ben nog op zoek naar de contactpersoon van de nbv die eerder technische ondersteuning aanbood aan EK/ TK
5.1.2.e
16:41
5.1.2.e
Zoals zojuist aan de telefoon besproken, deze mail is ter verificatie.
De CISO kan contact met ons opnemen op de volgende nummers: 5.1.2.e of 5.1.2.e
Met vriendelijke groet,
5.1.2.e
8
5.1.2.e


vodafone NL
22:09
Coördinatie ID-Ware
5.1.2.e
zo 2 okt.
5.1.2.e
5.1.2.e
Zoals zojuist aan de telefoon besproken, deze mail is ter verif...
Dit zijn de gegevens
5.1.2.e
5.1.2.e
16:42
5.1.2.e
En maandag om 11:00 uur organiseert het ncsc operationeel overleg met oa 5.1.2.e . Kunnen 5.1.2.e
5.1.2.e
5.1.2.e ook aansluiten?
16:44
5.1.2.e
5.1.2.e
Ja ik kan (5.1.2.e)
16:45
8
5.1.2.e
5.1.2.e
Dank je


vodafone NL
22:09
Coördinatie ID-Ware
5.1.2.e
5.1.2.e
Ja ik kan (5.1.2.e
zo 2 okt. 45
5.1.2.e
5.1.2.e
Dank je
16:45
5.1.2.e
Ik ook 5.1.2.e
email
5.1.2.e @tweedekamer.nl
Dit voor vergaderverziek
5.1.2.e
Verzoek
16:47
5.1.2.e
Mijn mailadres is
5.1.2.e @eerstekamer
5.1.2.e
.nl
16:48
5.1.2.e
Kreeg zojuist dit bericht...
8
Hoi 5.1.2.e, ik wil je melden dat

vodafone NL 22:09

Coördinatie ID-Ware

5.1.2.e .nl

16:48

zo 2 okt.

5.1.2.e

Kreeg zojuist dit bericht...

Hoi 5.1.2.e ik wil je melden dat blijkt dat wel gegevens zij gelekt van Belastingdienst medewerkers. Vanuit het project thuisbezorgen Rijkspas zijn er bij IDWare afleverdocumenten geleverd. Betreft digitale documenten met naam, rijkspasnummer en handtekening. Ik ga dit ook melden bij de Belastingdienst. De analyse is niet afgerond maar ik wilde dit wel melden.

5.1.2.e

17:00

5.1.2.e

Ok. Als dit voor onze communicatie iets betekent, graag info.

5.1.2.e

17:02

8


vodafone NL
22:09
Coördinatie ID-Ware
5.1.2.e
zo 2 okt.
Ik heb aangeven dat 5.1.2.e coördinatie doet...er zijn zoveel losse puzzelstukken en ik vind het raar dat nu nog steeds niet duidelijk welke bestanden of informatie verdwenen is...ze kunnen toch sowieso zien in welke bestanden er 'geshopt' is en nu zijn we meer dan een week verder en nog niks concreets
17:05
5.1.2.e
Herken het gevoel. Maar zijn wel 70k bestanden.
17:06
5.1.2.e
5.1.2.e
En maandag om 11:00 uur organiseert het ncsc operatione...
Kan de 5.1.2.e morgen ook aansluiten om 11:00 uur? En zo
8


vodafone NL
22:09
Coördinatie ID-Ware
5.1.2.e
En maandag zo 2 okt. uur
organiseert het ncsc operatione...
Kan de 5.1.2.e morgen ook aansluiten om 11:00 uur? En zo ja, dan graag een emailadres waar de uitnodiging naar toe kan.
5.1.2.e
5.1.2.e
18:14
5.1.2.e
5.1.2.e @minbzk.nl
5.1.2.e
Jahoor 18:18
5.1.2.e
Dank je 18:30
Zoals bekend opereert IDWare ook in Duitsland. Het NCSC onderhoudt contacten met de Duitse 'NCSC' over de digitale aanval
8

vodafone NL 22:09

Coördinatie ID-Ware

Zoals bekend opereert IDWare ook in Duitsl[redacted] NCSC onderhoudt contacten met de Duitse 'NCSC' over de digitale aanval.

zo 2 okt.

Naar aanleiding van de vandaag geschetste verwachting dat klanten in Duitsland op korte termijn geïnformeerd gaan worden, heeft het NCSC woordvoering JenV een update gestuurd. Deze staat in nauw contact met woordvoering BZK.

Waar nodig en mogelijk stemmen we ook af met onze Duitse collega's hierover. 21:39

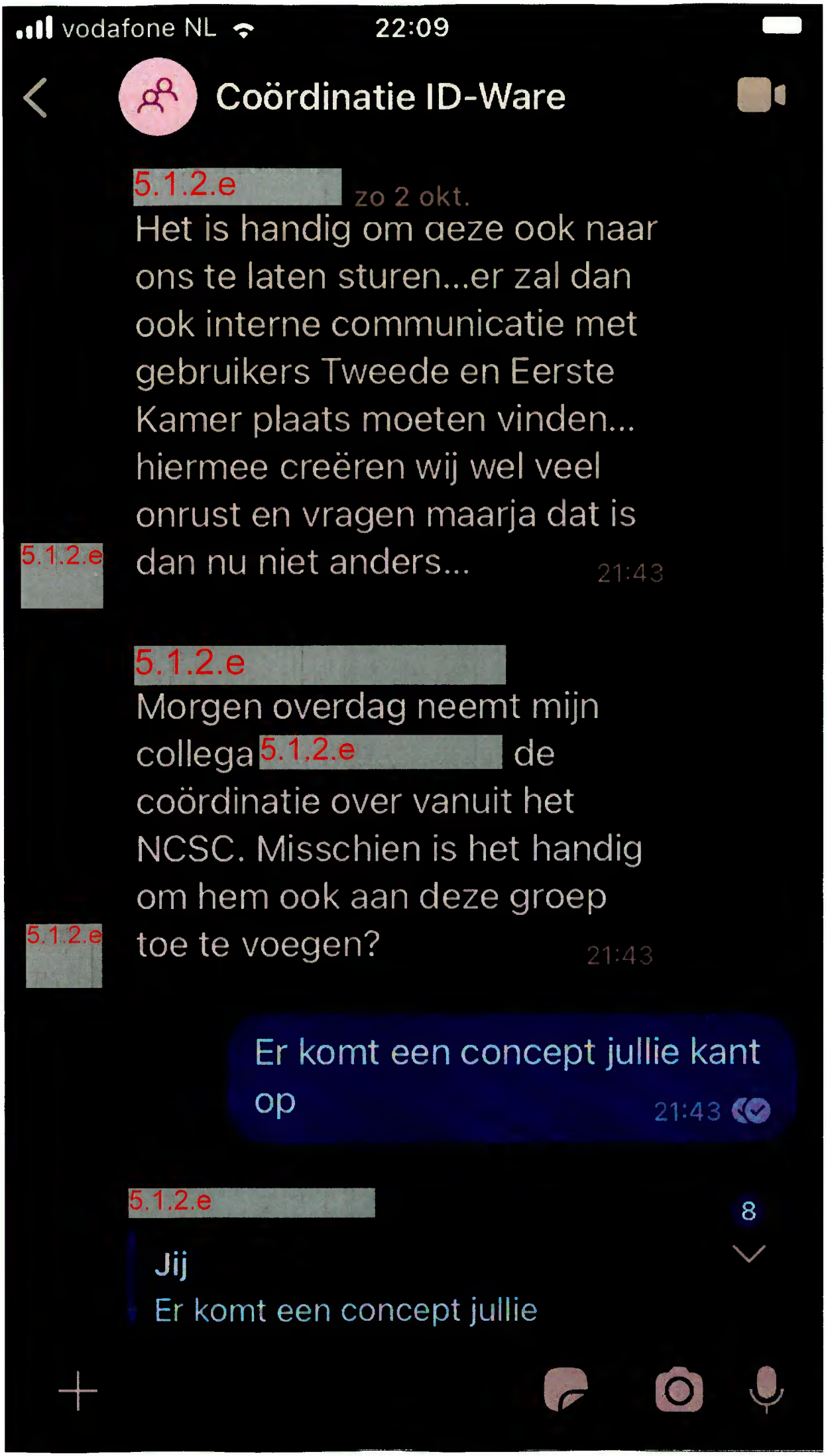
5.1.2.e

5.1.2.e heeft zijn of haar profielnaam van 5.1.2.e naar 5.1.2.e gewijzigd.

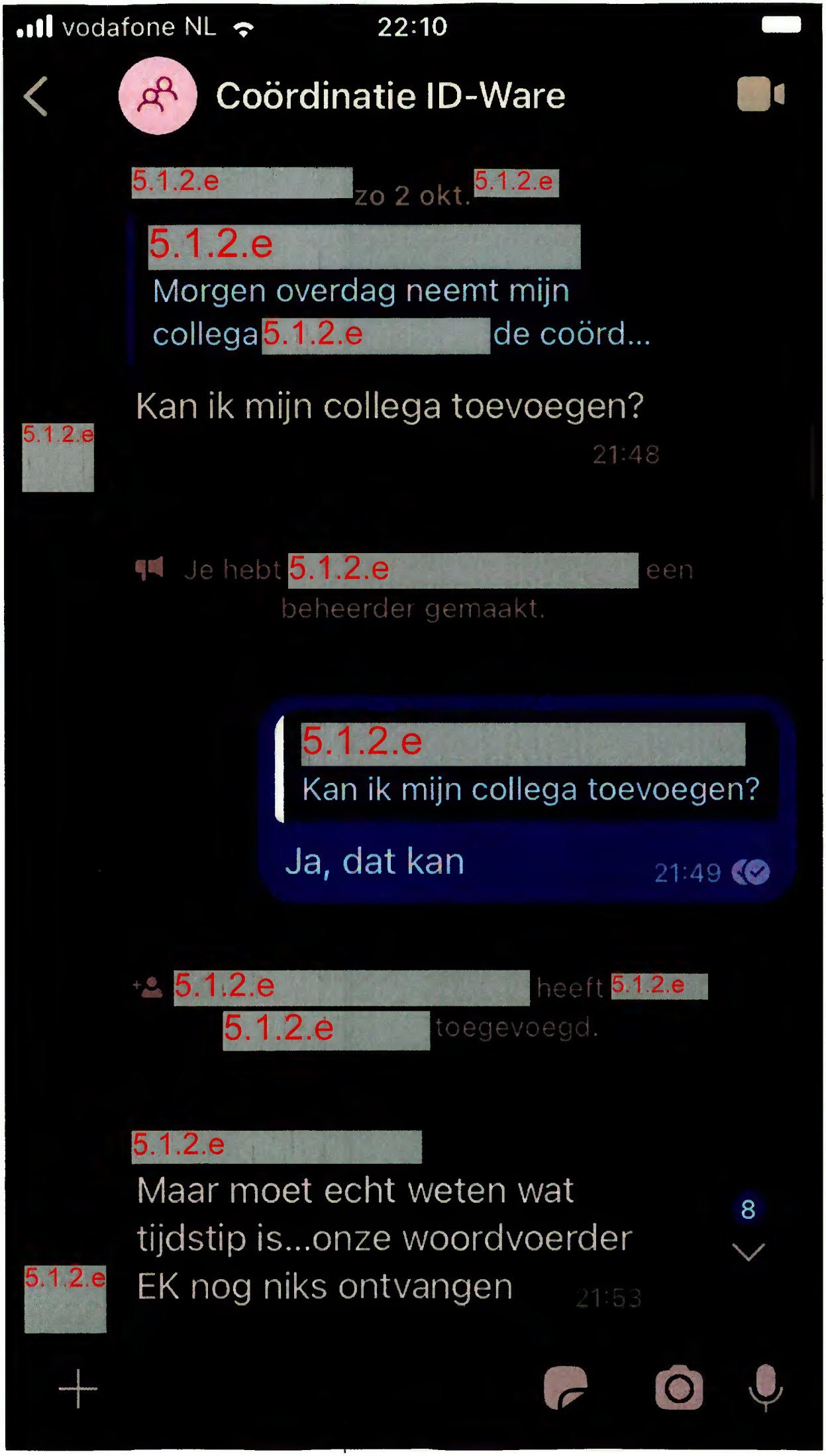
Contactpersoon bijwerken

8


vodafone NL
22:09
Coördinatie ID-Ware
5.1.2.e heeft zijn of haar profielnaam van 5.1.2.e zo 2 okt. 5.1.2.e gewijzigd.
Contactpersoon bijwerken
5.1.2.e
Dat moet dan ook naar woordvoering Tweede en
5.1.2.e
Eerste Kamer 21:40
5.1.2.e
Als woordvoering EK en TK nog niet in afstemming staan met BZK ondersteun ik dat van
5.1.2.e
harte 21:41
De contactgegevens zijn gedeeld met NCSC 21:43
5.1.2.e
Contactinfo woordvoerders EK
5.1.2.e
en TK is gisteren gedeeld 21:43
8
5.1.2.e


vodafone NL
22:09
Coördinatie ID-Ware
5.1.2.e
zo 2 okt.
Het is handig om deze ook naar ons te laten sturen...er zal dan ook interne communicatie met gebruikers Tweede en Eerste Kamer plaats moeten vinden... hiermee creëren wij wel veel onrust en vragen maarja dat is
5.1.2.e
dan nu niet anders...
21:43
5.1.2.e
Morgen overdag neemt mijn collega 5.1.2.e de coördinatie over vanuit het NCSC. Misschien is het handig om hem ook aan deze groep
5.1.2.e
toe te voegen?
21:43
Er komt een concept jullie kant op
21:43
5.1.2.e
8
Jij
Er komt een concept jullie


vodafone NL
22:10
Coördinatie ID-Ware
5.1.2.e
zo 2 okt.
Jij
Er komt een concept jullie kant op
Fijn! Al duidelijk wanneer (tijdstip / dag?) men wil gaan communiceren?
21:44
5.1.2.e
Jij
De contactgegevens zijn gedeeld met NCSC
Ook van EK/TK?
21:45
5.1.2.e
Ja
21:45
5.1.2.e
Michael Meijerink (Mobiel)
Morgen overdag neemt mijn collega Stefan Nelwan de coörd...
8
Kan ik mijn collega toevoegen?
5.1.2.e


vodafone NL
22:10
Coördinatie ID-Ware
5.1.2.e
zo 2 okt.
5.1.2.e
5.1.2.e
Morgen overdag neemt mijn collega 5.1.2.e de coörd...
Kan ik mijn collega toevoegen?
5.1.2.e
21:48
Je hebt 5.1.2.e een beheerder gemaakt.
5.1.2.e
Kan ik mijn collega toevoegen?
Ja, dat kan
21:49
5.1.2.e heeft 5.1.2.e 5.1.2.e toegevoegd.
5.1.2.e
Maar moet echt weten wat tijdstip is...onze woordvoerder EK nog niks ontvangen
8
5.1.2.e
21:53


vodafone NL
22:10
Coördinatie ID-Ware
5.1.2.e
Maar moet e zo 2 okt. n wat tijdstip is...onze woordvoerder EK nog niks ontvangen
21:53
5.1.2.e
Het is cruciaal dat dit goed tussen de woordvoerders (NCSC, TK, EK) wordt afgestemd. Dit gaat in crises vaak mis. Dat moeten we voorkomen.
22:01
5.1.2.e
Eens...woordvoerder EK (5.1.2.e) is morgenvroeg aanwezig voor goede afstemming intern en extern
22:03
5.1.2.e
Eens. Woordvoering JenV stemt intern af met NCSC en NCTV. JenV heeft met BZK collega al afstemming. Ik heb gevraagd morgenochtend ook
8


vodafone NL
22:10
Coördinatie ID-Ware
5.1.2.e
zo 2 okt.
Eens. Woordvoering JenV stemt intern af met NCSC en NCTV. JenV heeft met BZK collega al afstemming. Ik heb gevraagd morgenochtend ook woordvoering EK en TK aan te haken.
5.1.2.e
Wie is woordvoerder TK
22:07
5.1.2.e
5.1.2.e
Is al gedeeld met NCSC
22:07
5.1.2.e
5.1.2.e
Dank je
22:09
5.1.2.e
Bij EK is dat 5.1.2.e , 5.1.2.e
5.1.2.e
5.1.2.e
22:11
5.1.2.e
5.1.2.e
5.1.2.e
woordvoering
8


vodafone NL
22:10
Coördinatie ID-Ware
5.1.2.e
Bij EK is dat zo 2 okt. 5.1.2.e, 5.1.2.e
5.1.2.e
5.1.2.e
22:11
5.1.2.e
5.1.2.e
5.1.2.e woordvoering
TK
Wij moeten daar niet tussen zitten als deze groep. Hierover moeten de betrokken woordvoerders met elkaar schakelen. Anders krijg je ruis op de lijn.
5.1.2.e
22:13
5.1.2.e
Ik laat gegevens zsm doorsturen aan betrokken woordvoerder JenV
5.1.2.e
22:15
5.1.2.e
Ok
Misschien kunnen de woordvoerders een eigen
8


vodafone NL
22:10
Coördinatie ID-Ware
5.1.2.e
zo 2 okt.
Ok
Misschien kunnen de woordvoerders een eigen signalgroep inrichten, als dat nog niet is gebeurd.
22:18
Ik hoor net dat er nog niemand contact heeft gelegd met onze woordvoerder, ook gisteren niet. Zij weet ook niet wie zij bij NCSC moet contacten.
5.1.2.e
22:57
ma 3 okt.
5.1.2.e
Woordvoerders
JenV
5.1.2.e
Mobiel: 5.1.2.e
E-mail: 5.1.2.e @minjenv.nl
8


vodafone NL
22:10
Coördinatie ID-Ware
5.1.2.e
Woordvoerc ma 3 okt.
JenV
5.1.2.e
Mobiel: 5.1.2.e
E-
mail: 5.1.2.e
BZK
5.1.2.e
woordvoerder
5.1.2.e
5.1.2.e @minbzk.nl
5.1.2.e
06:55
5.1.2.e
5.1.2.e
Thx 07:45
5.1.2.e
5.1.2.e , de 5.1.2.evan
IDWare is bereid om op afstand
8

vodafone NL 22:10

Coördinatie ID-Ware

5.1.2.e

ma 3 okt.

5.1.2.e , de 5.1.2.e van IDWare is bereid om op afstand aan te sluiten bij het overleg om 11:00 10:19

5.1.2.e

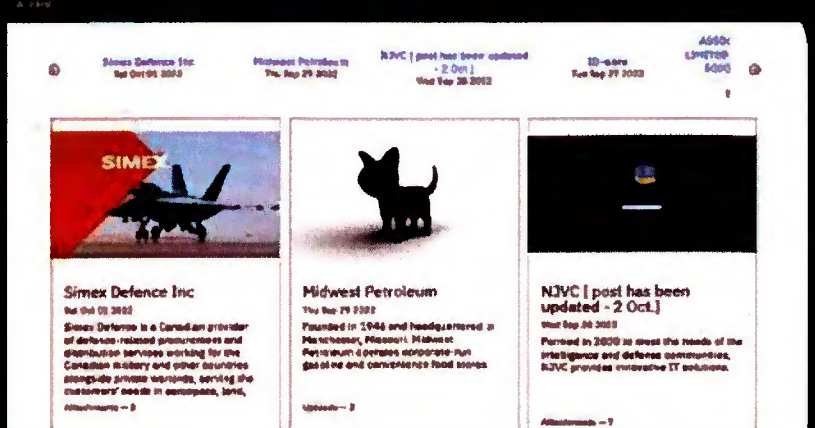
5.1.2.e Ok 10:22

5.1.2.e

Van 11.00 tot 12.30 is operationeel overleg. 5.1.2.e is wel bereikbaar 10:47

5.1.2.e

@all, leaksite is weer onine. Nieuwe bedrijven die gehackt. Geen aanvullingen op IDWare.



8

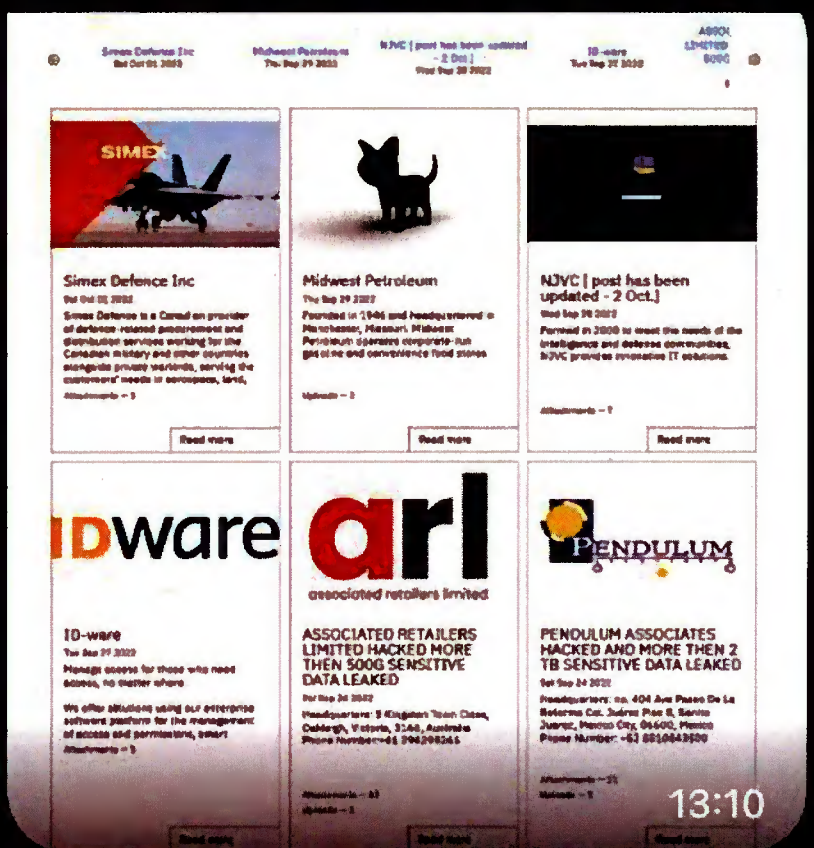
vodafone NL 22:10

Coördinatie ID-Ware

5.1.2.e

ma 3 okt.

@all, leaksite is now online.
Nieuwe bedrijven die gehackt.
Geen aanvullingen op IDWare.



5.1.2.e

5.1.2.e

Dank je. Ik neem het mee in het informatie beeld

14:28

Vanuit het NCSC zullen we deze signal groep een paar keer per dag monitoren.

8


vodafone NL
22:10
Coördinatie ID-Ware
ma 3 okt.
Vanuit het N ,n we deze signal groep een paar keer per dag monitoren.
Voor dringende vragen of meldingen graag telefonisch contact of per e-mail naar
5.1.2.e
CERT@NCSC.NL
16:31
5.1.2.e
Ik zie via verslag woordvoerders dat beeld is dat ook de EErste en tweede kamer geraakt zijn. Is hier iets meer over te melden?
5.1.2.e
20:47
5.1.2.e
Dag @5.1.2.e , ik ben 5.1.2.e
5.1.2.e en monitor deze groep ipv 5.1.2.e
8
"Geraakt" lijkt me inderdaad wat sterk uitgedrukt. Ik zoek

vodafone NL 22:10

Coördinatie ID-Ware

5.1.2.e

Dag @5.1.2.e, ik ben 5.1.2.e 5.1.2.e en monitor deze groep ipv 5.1.2.e

"Geraakt" lijkt me inderdaad wat sterk uitgedrukt. Ik zoek het uit. 20:53

5.1.2.e

5.1.2.e

Fijn dank je 20:53

5.1.2.e

Overigens, morgen staat op ons programma dat we samen met ID-ware en de betrokken IR-partij gaan kijken naar welke soorten data zijn gelekt. Als daar iets uitkomt, dan zullen we dit ook delen. 20:58

5.1.2.e

8

Hoor graag nog wel even over dat 'geraakt'...volgens mij


vodafone NL
22:10
Coördinatie ID-Ware
ma 3 okt.
@5.1.2.e ik heb ook aan de cert-box nog wat info gestuurd vanuit Rijkspasbeheer.
5.1.2.e heeft vanuit een vakantieadres rechtstreeks met ID-w geschakeld, de info die ik hierover kreeg heb ik gedeeld.
Ik maak nog even een wrap-up van vandaag voor onze tijdlijn
21:04
5.1.2.e
5.1.2.e
Hoor graag nog wel even over dat 'geraakt'...volgens mij onjuist
Ik zie dat ik het verslag niet heb van de woordvoerders.
Waarschijnlijk zit deze in de mailbox bij communicatie.
5.1.2.e
Vraag het morgen na.
8


vodafone NL
22:10
Coördinatie ID-Ware
5.1.2.e
Vraag het m
ma 3 okt.
21:08
5.1.2.e
5.1.2.e en ik weten niets over eventuele voorlichting, de reden waarom, etc. NCTV heeft wel contact gehad met 5.1.2.e 5.1.2.e . Ook 5.1.2.e 5.1.2.e is verbaasd.
Te veel aparte lijntjes maken het er niet duidelijk op.
Volgens mij zouden wij deze signalgroep gebruiken voor de communicatie tussen NCSC en EK/ TK. Zeker aks het gaat om aanleiding voor communicatie. Dat is een sleutelbesluit.
En over de inhoud van communicatie kunnen de betrokken woordvierders overleggen.
5.1.2.e
21:13
8
5.1.2.e


vodafone NL
22:11
Coördinatie ID-Ware
5.1.2.e
ma 3 okt.
Wat ik heb ka
cert@ncsc.nl mailen als je wil
5.1.2.e Of ergens anders
naartoe
21:17
5.1.2.e
Het idee bij een overleg bij de NCTV was dat de woordvoeringslijnen zouden worden afgestemd tussen alle woordvoerders. Dit heeft zo te zien geleid tot verwarring.
Ik probeer onze betrokken woordvoerder te bereiken, maar heb nog geen contact kunnen maken.
5.1.2.e
Wat ik heb kan ik naar cert@ncsc.nl mailen als je wil 5.1.2.e
Cert@ncsc.nl is
21:23
8
5.1.2.e

vodafone NL 22:11

Coördinatie ID-Ware

5.1.2.e ma 3 okt.

Heb verslag net gehad. @5.1.2.e dank hiervoor. Daarin staat dat de Kamers en de Belastingdienst zijn geraakt. Dat wekt verwarring. De hele overheid is geraakt, maar het is nog niet gebkeken dat data van EK/TK op straat ligt. 21:26

5.1.2.e

5.1.2.e

5.1.2.e corrigeert intern communicatie EK hierop..verstandig om dat ook bij TK te doen..

En mbt Belastingdienst zijn er natuurlijk wel 3500 gegevens gelekt maar dat kwam weer door het thuisbezorgen van de rijkspas 21:30

5.1.2.e

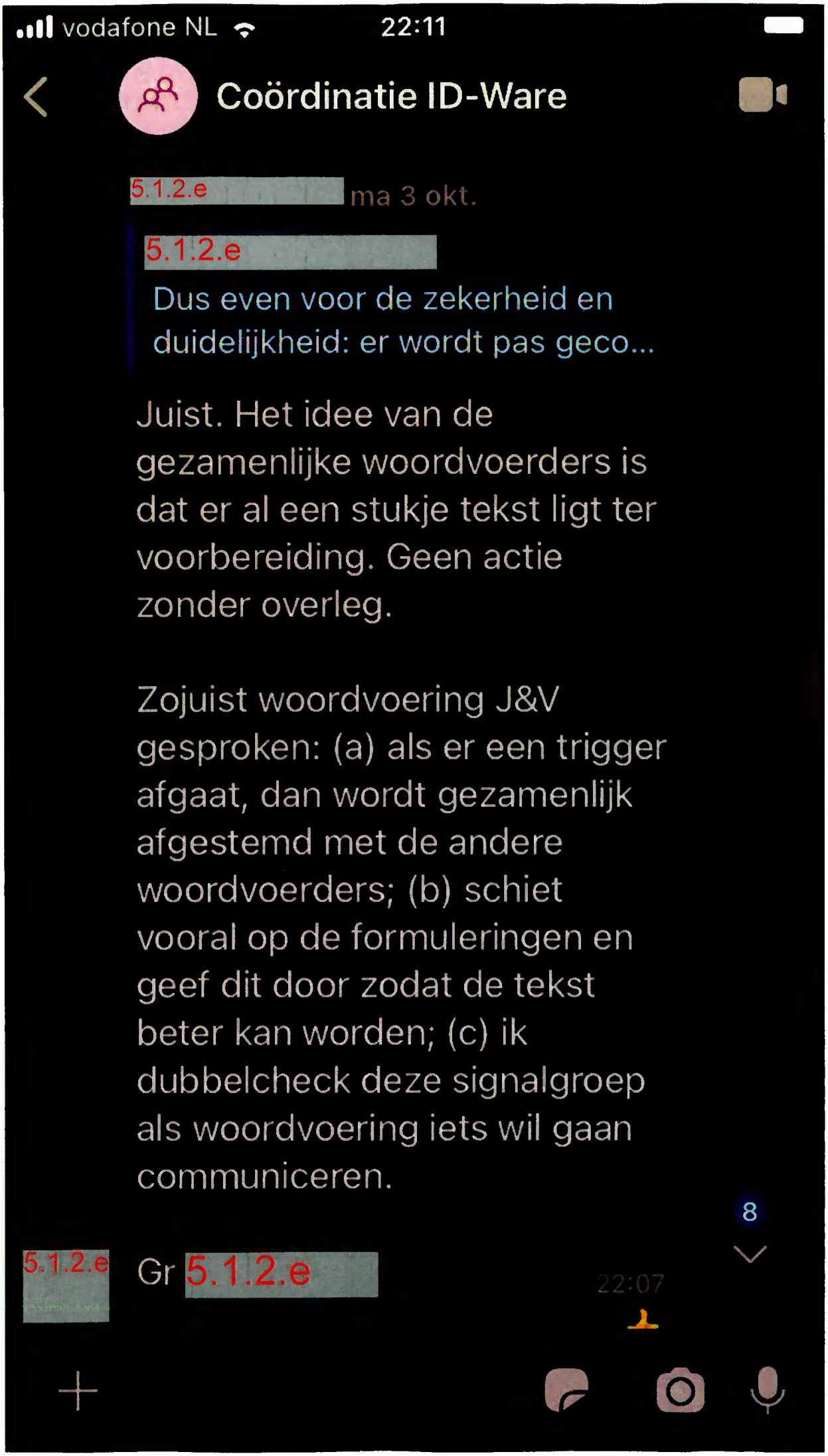
8

5.1.2.e

Mail ontvangen en gelezen Wat


vodafone NL
22:11
Coördinatie ID-Ware
5.1.2.e
ma 3 okt.
Mail ontvangen en gelezen. Wat ik heb ontvangen is een afgestemde woordvoeringslijn voor 3 scenario's die worden gebruikt als er een bepaalde trigger is. Deze triggers spelen (nog) niet.
21:44
5.1.2.e
Precies!
21:44
5.1.2.e
Mooi dank je
21:45
5.1.2.e
Fijn dat jullie zo scherp zijn. Ik koppel het terug aan woordvoering en zal morgen jullie gedurende de dag op de hoogte houden.
21:47
8
Jij
5.1.2.e

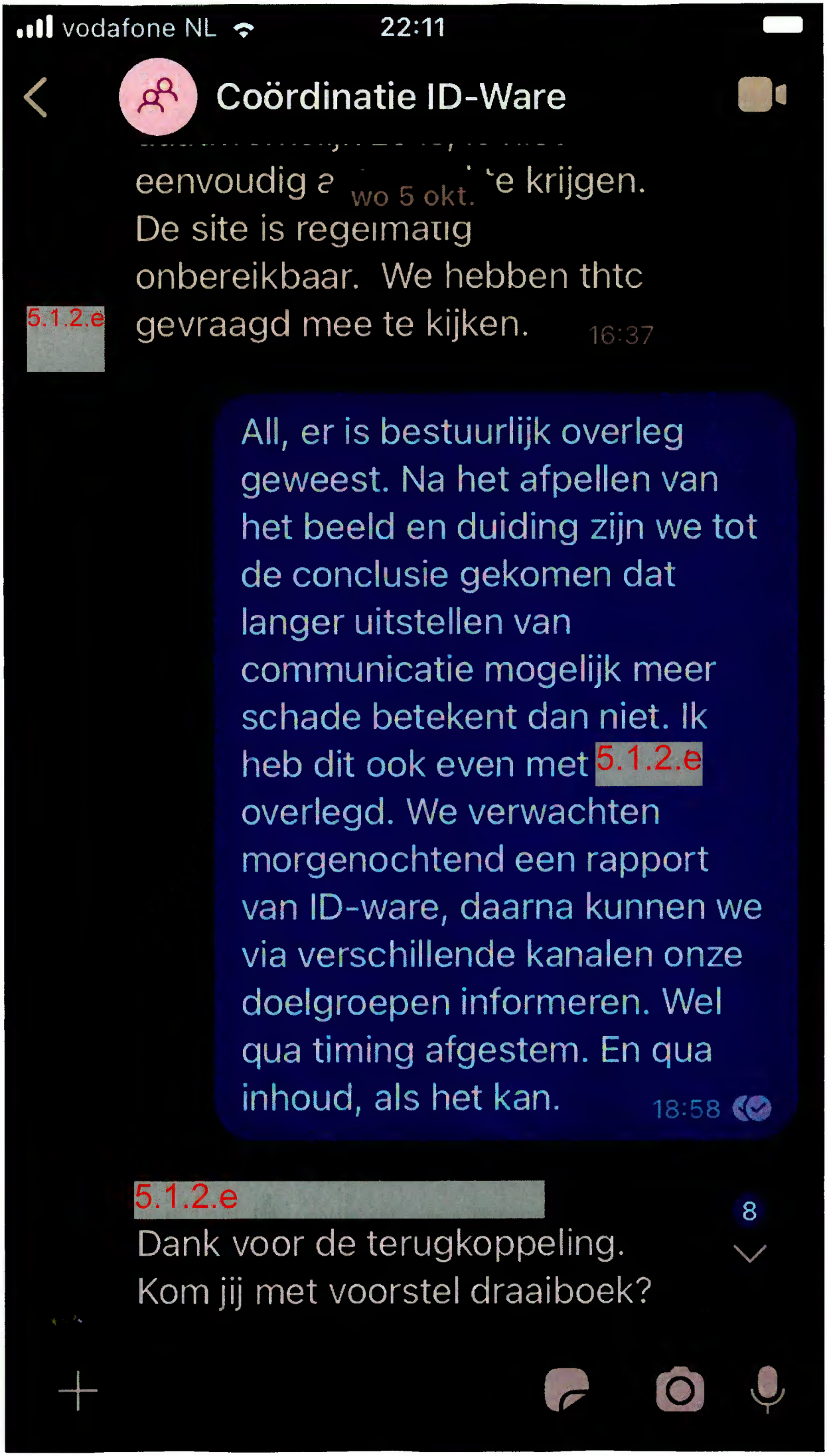

vodafone NL
22:11
Coördinatie ID-Ware
Jij
ma 3 okt.
@5.1.2.e ik heb ook aan de cert-box nog wat inf...
5.1.2.e
Mail gezien, dank!
21:48
5.1.2.e
5.1.2.e
Mail ontvangen en gelezen. Wat ik heb ontvangen is een afgeste...
Dus even voor de zekerheid en duidelijkheid: er wordt pas gecommuniceerd als er een trigger is, deze trigger speelt nog niet, du morgen wordt er niet gecommuniceerd?
5.1.2.e
21:54
5.1.2.e
5.1.2.e
Dus even voor de zekerheid en duidelijkheid: er wordt pas geco...
8
Juist. Het idee van de gezamenlijke woordvoerders is


vodafone NL
22:11
Coördinatie ID-Ware
5.1.2.e
ma 3 okt.
5.1.2.e
Dus even voor de zekerheid en duidelijkheid: er wordt pas geco...
Juist. Het idee van de gezamenlijke woordvoerders is dat er al een stukje tekst ligt ter voorbereiding. Geen actie zonder overleg.
Zojuist woordvoering J&V gesproken: (a) als er een trigger afgaat, dan wordt gezamenlijk afgestemd met de andere woordvoerders; (b) schiet vooral op de formuleringen en geef dit door zodat de tekst beter kan worden; (c) ik dubbelcheck deze signalgroep als woordvoering iets wil gaan communiceren.
8
5.1.2.e
Gr 5.1.2.e
22:07


vodafone NL
22:11
Coördinatie ID-Ware
Bijgewerkte tijdlijn in de mail. Ik maak voor morgen eind van de dag een Webex voor als er ontwikkelingen zijn
22:12
2
ma 3 okt.
di 4 okt.
5.1.2.e
We hebben maandag kort gesproken over afstemmen tussen het security team EK/TK en NCSC.
Als dat nog steeds wenselijk en mogelijk is, zou ik graag de contactgegevens ontvangen van degene met wie wij contact op kunnen nemen.
18:50
5.1.2.e
5.1.2.e
5.1.2.e
5.1.2.e
5.1.2.e
5.1.2.e
20:20
8


vodafone NL
22:11
Coördinatie ID-Ware
di 4 okt.
5.1.2.e
5.1.2.e
Dank je
20:20
5.1.2.e
5.1.2.e
Ik laat het graag bij 5.1.2.e
21:12
wo 5 okt.
5.1.2.e
@5.1.2.e, volg jij AO vanmiddag of er wel/niet vragen worden gesteld over IDWare bij het AO. Zoja dan moeten we ook gaan communiceren...gr 5.1.2.e
5.1.2.e
10:53
5.1.2.e
@5.1.2.e
Graag contact opnemen met 5.1.2.e . Wij hebben sterke aanwijzingen dat er diverse data van ons is gelekt. Oa van 5.1.2.e
5.1.2.e
14:22
8
5.1.2.e


vodafone NL
22:11
Coördinatie ID-Ware
5.1.2.e
Er wordt nu wo 5 okt. ,:26
5.1.2.e
Prima 14:32
5.1.2.e
Ook graag hier dan signaal (terug) of dit daadwerkelijk zo is of anders is..dus graag feitelijkheid vaststellen in relatie tot hack IDWare 14:34
5.1.2.e
Gesprek is geweest met 5.1.2.e
We starten onderzoek. 15:02
5.1.2.e
Ook graag hier dan signaal (terug) of dit daadwerkelijk zo i...
Op de vraag of dit daadwerkelijk zo is, is niet eenvoudig antwoord te krijgen.
De site is regelmatig
8


vodafone NL
22:11
Coördinatie ID-Ware
eenvoudig a
wo 5 okt.
'e krijgen.
De site is regelmatig onbereikbaar. We hebben thtc
5.1.2.e
gevraagd mee te kijken.
16:37
All, er is bestuurlijk overleg geweest. Na het afpellen van het beeld en duiding zijn we tot de conclusie gekomen dat langer uitstellen van communicatie mogelijk meer schade betekent dan niet. Ik heb dit ook even met 5.1.2.e overlegd. We verwachten morgenochtend een rapport van ID-ware, daarna kunnen we via verschillende kanalen onze doelgroepen informeren. Wel qua timing afgestem. En qua inhoud, als het kan.
18:58
5.1.2.e
Dank voor de terugkoppeling.
Kom jij met voorstel draaiboek?
8

vodafone NL 22:11

Coördinatie ID-Ware

5.1.2.e wo 5 okt.

> Jij
> All, er is bestuurlijk overleg geweest. Na het afpellen van he...

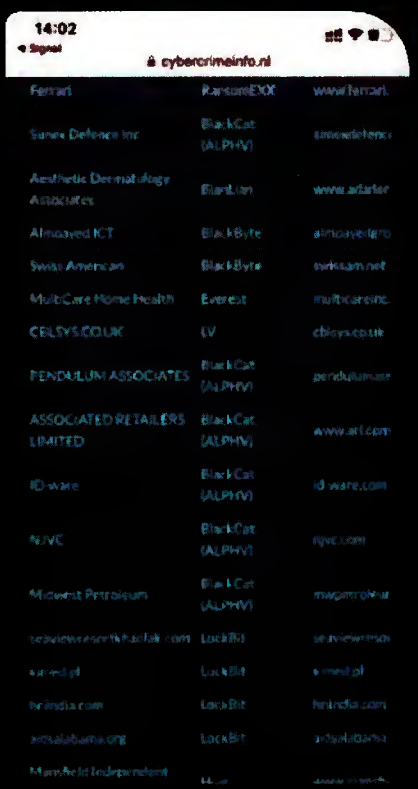
Heb je al beeld hoelaat dit rapport van ID komt? Dan stemmen wij onze interne crisis structuur daarop af

5.1.2.e 19:59

do 6 okt.

5.1.2.e

Deze staat op internet



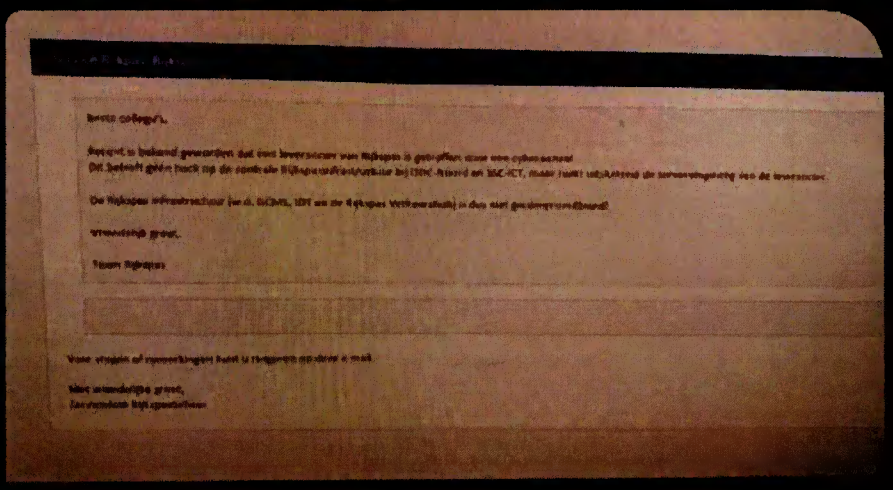
8


vodafone NL
22:12
Coördinatie ID-Ware
Allen, zojuis do 6 okt. at met het NCSC. Het NCSC bevestigd onze bevindingen. Zij hebben de persoonsgegevens ook gezien. Op basis van onze link hebben zij vannacht 1.000 links naar binnen gehaald en daar is meer data gevonden. Een nieuw item is dat er data is gevonden over onze kaartlezers. Het NCSC onderzoekt nu wat deze data is en of er encryptie sleutels tussen zitten. Het NCSC is groot opgeschaald. Ik werd nogmaals bedankt voor de verstrekte info.
Bericht van 5.1.2.e
Om 14.45 uur komt ons CT bij elkaar
8
Rijkspasbeheer heeft met zijn afnemers gecommuniceerd

vodafone NL 22:12

Coördinatie ID-Ware

Rijkspasbeheer heeft met zijn afnemers ge do 6 okt. ceerd



5.1.2.e Ook niet handig 14:09

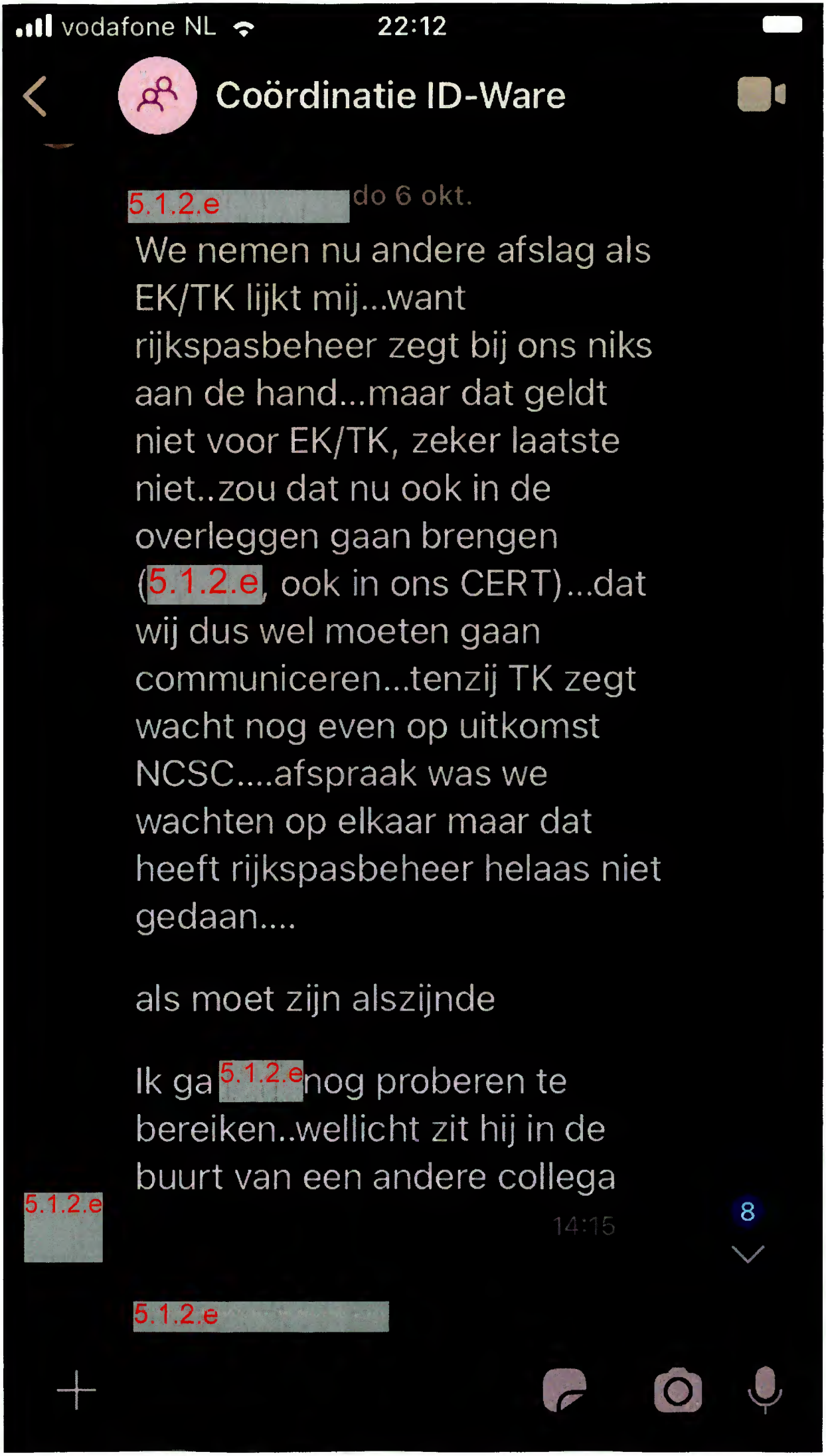
5.1.2.e
Zeker niet handig.

Dit versnelt noodzaak tot verdere communicatie lijkt mij.

5.1.2.e 14:09

5.1.2.e
We nemen nu andere afslag als EK/TK lijkt mij...want rijkspasbeheer zegt bij ons niks aan de hand...maar dat geldt niet voor EK/TK, zeker laatste niet..zou dat nu ook in de

8


vodafone NL
22:12
Coördinatie ID-Ware
5.1.2.e
do 6 okt.
We nemen nu andere afslag als EK/TK lijkt mij...want rijkspasbeheer zegt bij ons niks aan de hand...maar dat geldt niet voor EK/TK, zeker laatste niet..zou dat nu ook in de overleggen gaan brengen (5.1.2.e, ook in ons CERT)...dat wij dus wel moeten gaan communiceren...tenzij TK zegt wacht nog even op uitkomst NCSC....afspraak was we wachten op elkaar maar dat heeft rijkspasbeheer helaas niet gedaan....
als moet zijn alszijnde
Ik ga 5.1.2.e nog proberen te bereiken..wellicht zit hij in de buurt van een andere collega
5.1.2.e
14:15
8
5.1.2.e


vodafone NL
22:12
Coördinatie ID-Ware
5.1.2.e
do 6 okt.
Ik stel voor dat voor communicatie bij EK even op CT TK wachten. Wel bereiden we nu losse communicatie voor. Voor als er geen ruimte meer is om te wachten.
14:23
5.1.2.e
Ja lijkt mij goed...
14:24
5.1.2.e
ANP heeft bij ons de eerste persvraag gesteld
14:27
vr 7 okt.
Ik heb de brief de lijn in gestuurd, graag even een signaal als er naar medewerkers is gecommuniceerd, dan duwen we de brief
09:1
8
5.1.2.e


vodafone NL
22:12
Coördinatie ID-Ware
vr 7 okt.
Ik he f de lijn in gestuurd, graag even een signaal als er naar medewerkers is gecommuniceerd, dan duwen we de brief
09:18
5.1.2.e
hoi 5.1.2.e heb je laatste versie voor ons?
09:19
Excuus, ik dacht dat ik dat gisteravond had gedaan. Komt eraan
09:21
5.1.2.e
als het dezelfde versie is, dan niet nodig
09:21
5.1.2.e
Ok. Betekent dit dat wij kunnen communiceren?
Wij hebben over 5 minuten CT
8


vodafone NL
22:12
Coördinatie ID-Ware
vr 7 okt
5.1.2.e
Ok. Betekent dit dat wij kunnen communiceren?
Ja
09:23
5.1.2.e
als het dezelfde versie is, dan niet nodig
Hij zit in de mail bij de terugkoppeling van het beleidsovetleg met de NCTV
09:26
5.1.2.e
ik zag het, dank je
09:26
5.1.2.e
TK gaat vandaag rond dit tijdstip (12 uur) communiceren.
5.1.2.e en 5.1.2.e zijn telefonisch geïnformeerd hierover.
12:02
8


vodafone NL
22:12
Coördinatie ID-Ware
5.1.2.e
vr 7 okt.
TK gaat vandaag rond dit tijdstip (12 uur) communiceren. 5.1.2.e en 5.1.2.e EK zijn telefonisch geïnformeerd hierover.
12:02
5.1.2.e
5.1.2.e
Wij verzenden het op dit moment
12:15
5.1.2.e
5.1.2.e
Wij hebben verzonden
12:21
5.1.2.e
5.1.2.e
wij ook
12:33
5.1.2.e
Allen: NCSC wil in navolging van de publicatie van de kamerbrief onze doelgroepen informeren. We presenteren informatie in lijn met de Kamerbrief, maar bieden
8


vodafone NL
22:12
Coördinatie ID-Ware
5.1.2.e
Allen: NCSC vr 7 okt. volging van de publicatie van de kamerbrief onze doelgroepen informeren. We presenteren informatie in lijn met de Kamerbrief, maar bieden handelingsperspectief in de vorm van: als je klant ben van ID-Ware, inventariseer dan welke gegevens je hebt gedeeld en neem contact op met ID-ware of deze gegevens eventueel zijn gelekt.
Wij hebben dit afgestemd met ID-ware, want zij kunnen door hun klanten worden benaderd.
NB: ID-Ware was niet op de hoogte van de communicatie die de RO voorbere...
5.1.2.e
Meer lezen
12:50
8
5.1.2.e

vodafone NL 22:12

Coördinatie ID-Ware

5.1.2.e

vr 7 okt.

5.1.2.e

Allen: NCSC wil in navolging van de publicatie van de kamerbrief...

TK communiceert hierover niet met ID ware. Coördinatie ligt bij NCSC.

5.1.2.e

Dit ivm de NB opmerking 13:01

5.1.2.e

Krijgen wij een melding van jullie als de brief naar de Kamer is verzonden?

8

Data Kamerleden gelekt door

vodafone NL 22:12

Coördinatie ID-Ware

vr 7 okt.

Data Kamerleden gelekt door hack bij IT-bedrijf: gegevens toe...

Door een hack bij het bedrijf ID-ware zijn onder meer de gegevens van de toegangspassen van Twee...

www.volkskrant.nl · 7 okt. 2022

https://www.volkskrant.nl/nieuws-achtergrond/data-kamerleden-gelekt-door-hack-bij-it-bedrijf-gegevens-toegangspassen-online~b7051db9/

5.1.2.e

13:32

8

Buiten reikwijdte


vodafone NL
22:12
Coördinatie ID-Ware
Buiten reikwijdte
5.1.2.e
Buiten reikwijdte
5.1.2.e
20:29
5.1.2.e
Buiten reikwijdte
5.1.2.e
5.1.2.e
@5.1.2.elees even mijn bericht
aan jou in signal
20:33
5.1.2.e
En Security.nl een mooi
genuanceerd verhaal.
Volkskrant heeft artikel
aangepast na de brief.
8
20:3

vodafone NL 22:13

Coördinatie ID-Ware

5.1.2.e

Buiten reikwijdte

5.1.2.e

5.1.2.e

Het NCSC is beperkt benaderd. Het is ook rustig.

Wel via 5.1.2.e contact gehad met de 5.1.2.e . Issue is geadresseerd. 20:37

5.1.2.e

5.1.2.e

Er is contact geweest met ANP, NOS, RTL en Telegraaf. Allen om reeds verkregen (al dan niet vanuit Volkskrant) info te verifiëren. Alle betrokken woordvoerders verwijzen naar de kamerbrief. Vragen zijn binnengekomen bij zowel ons als BZK en NCSC. Daarmee de last verdeeld. De druk is

8

vodafone NL 22:13

Coördinatie ID-Ware

als BZK en N[redacted] armee de
vr 7 okt.
last verdeeld. De druk is inmiddels afgenomen na reactie van de staatssecretaris in het AD.

Bericht van onze voorlichters

Intern ook weinig reacties, slechts 2

In mailbox Bureau CISO TK

5.1.2.e

20:42

5.1.2.e

Vanuit BVA TK hebben wij vanuit de organisatie of vanuit Kamerleden ook nog geen vragen, bijzonderheden of verdachte situaties binnen gekregen.

5.1.2.e

20:42

5.1.2.e

Ook niet bij Beveiligingsdienst?

5.1.2.e

20:45

8

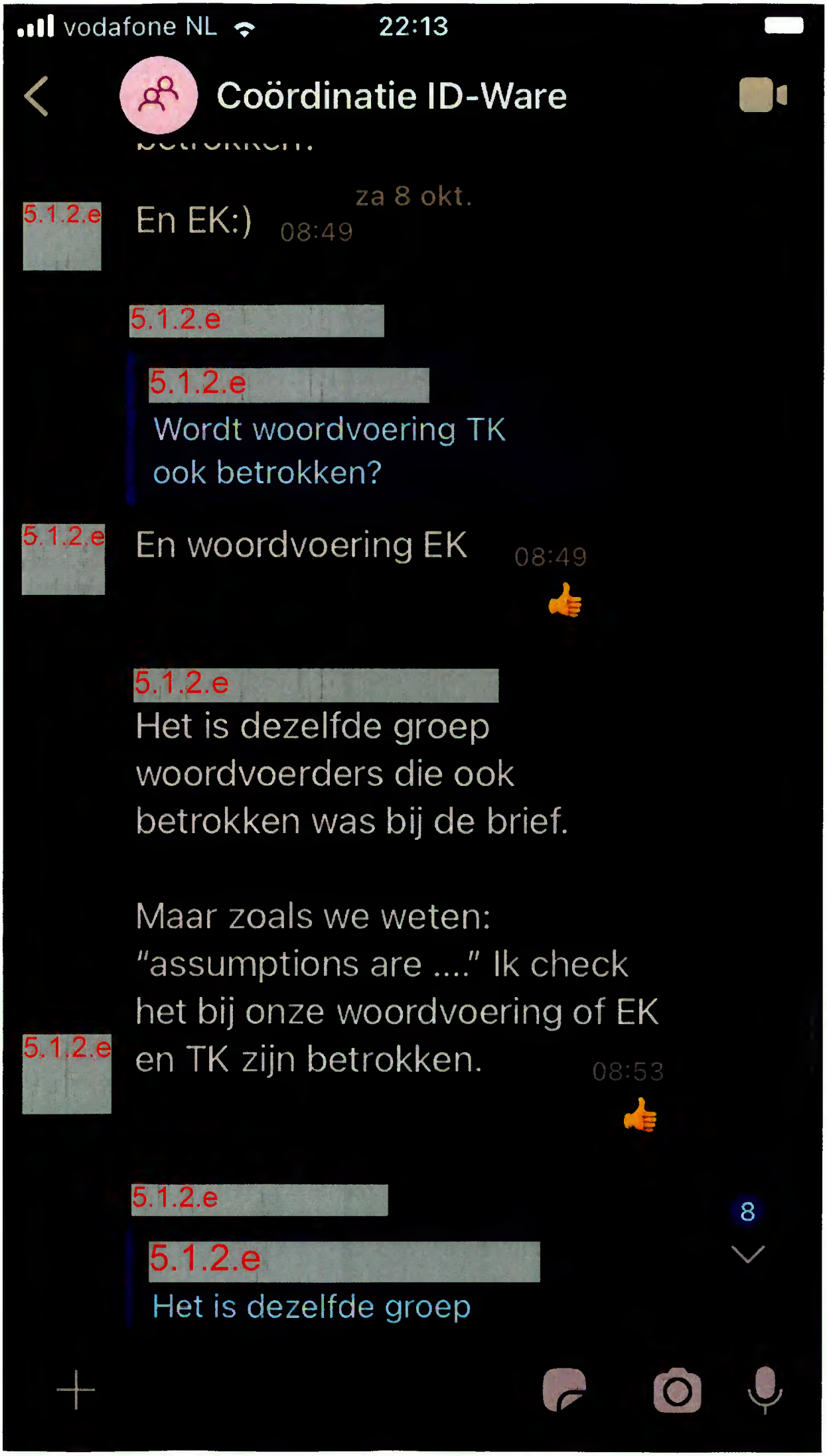

vodafone NL
22:13
Coördinatie ID-Ware
5.1.2.e
vr 7 okt.
Ook niet bij B...gsdienst?
20:45
5.1.2.e
Bij de balie wel een paar vragen van pashouders
20:47
5.1.2.e
5.1.2.e
Vanuit BVA TK hebben wij vanuit de organisatie of vanuit Kamerl...
Bij de eerste kamer tot nu toe ook geen reacties ontvangen.
20:47
5.1.2.e
Nou mooi allemaal..rustig weekend allen en dank voor goede samenwerking!
20:49
2
8
5.1.2.e
U2
20:51

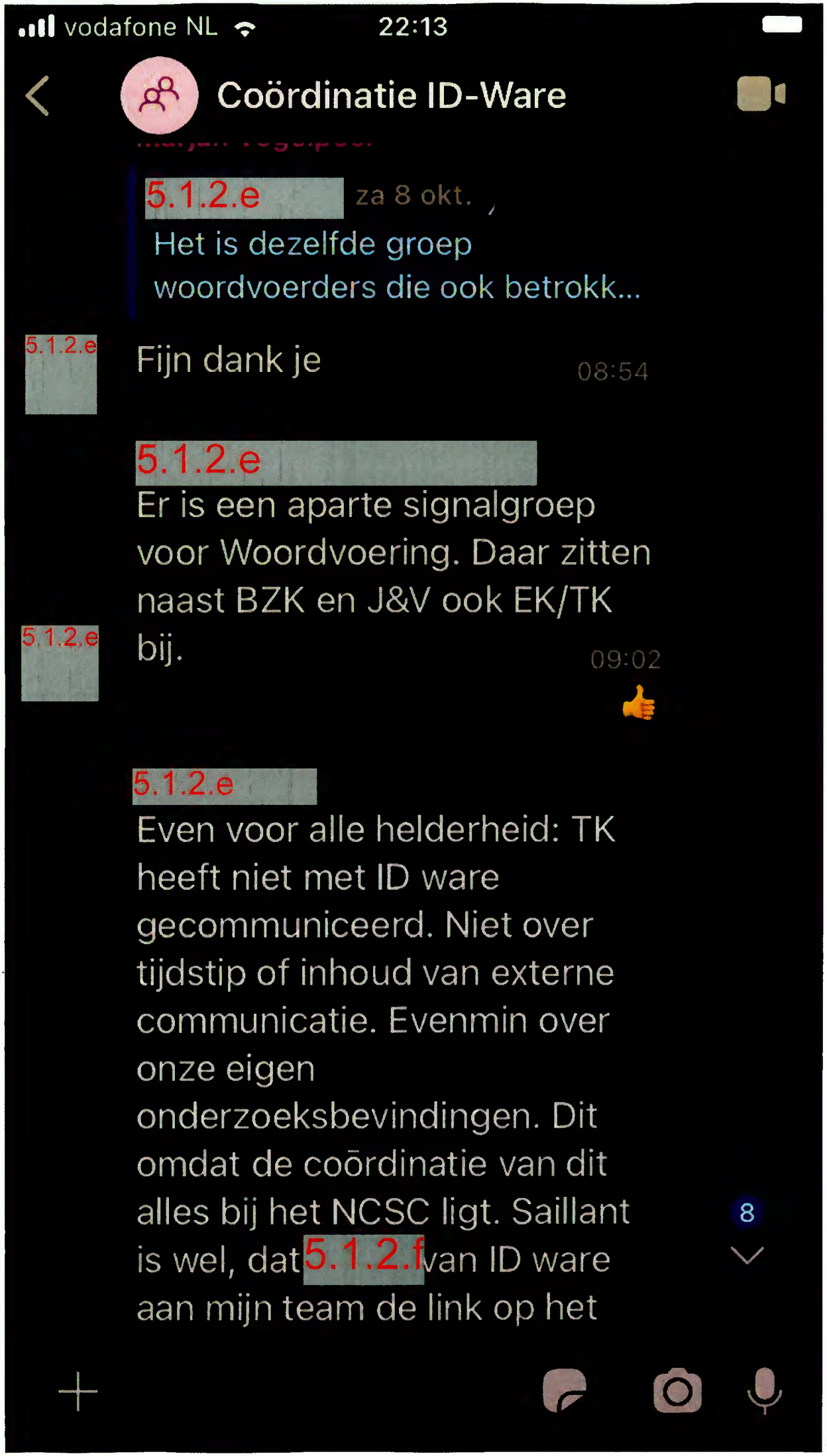

vodafone NL
22:13
Coördinatie ID-Ware
5.1.2.e
20:51
vr 7 okt.
5.1.2.e
Ik ben benieuwd of hackers/ security onderzoekers nog wat gaan vinden in de data (en rapporteren). NCSC monitort verschillende socials/blogs/etc.
Het NCSC eventteam is formeel nog intern opgeschaald. We verzamelen binnengekomen vragen, media/artikelen en kijken maandag naar de opbrengst, tenzij er natuurlijk iets bijzonders wordt gezien. Maandag waarschijnlijk afschalen.
5.1.2.e
21:11
za 8 okt.
Gehackt IT-bedrijf zegt dat gegevens Kamerleden niet zijn...
IT-toeleverancier ID-ware ontkent dat door een hack bij het bedrijf de
8

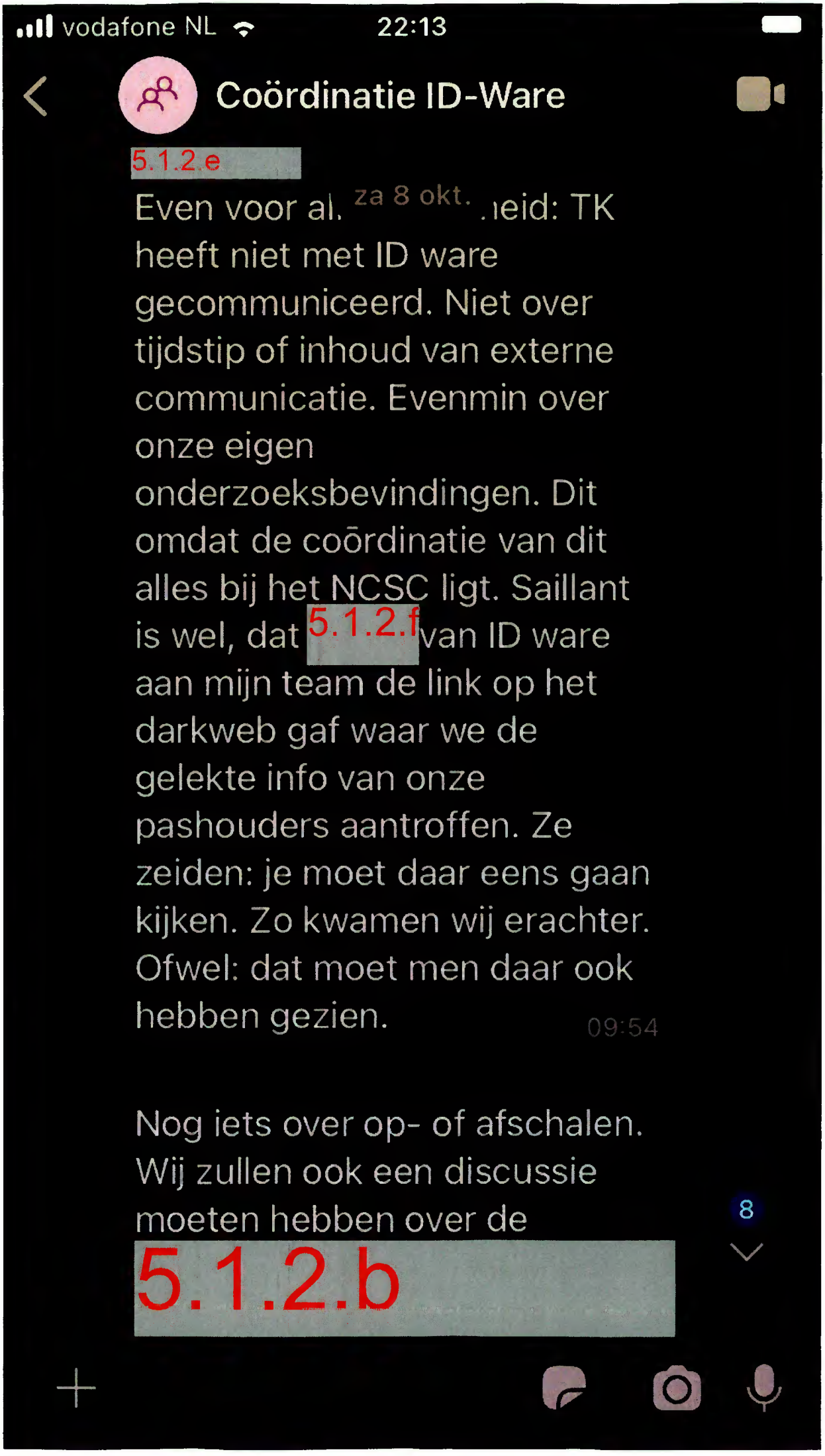

vodafone NL
22:13
Coördinatie ID-Ware
Gehackt IT-bedrijf zegt dat
gegevens Ka za 8 okt. niet zijn...
IT-toeleverancier ID-ware ontkent
dat door een hack bij het bedrijf de
persoonsgegevens van Eerste en...
www.nu.nl
5.1.2.e
https://www.nu.nl/tech/
6228618/gehackt-it-bedrijf-
zegt-dat-gegevens-
kamerleden-niet-zijn-
buitgemaakt.html
Goedemorgen,
Zie bericht: dit kan echt niet, zo
via media. Zouden jullie (5.1.2.e
5.1.2.e en NCSC) hier regie op
5.1.2.e willen (laten) plegen?
04:31
5.1.2.e
Goedemorgen, ja, wij hebben
dit ook gezien.
8
Ik heb gisteren om 13h contact


vodafone NL
22:13
Coördinatie ID-Ware
5.1.2.e
Goedemorg za 8 okt. hebben dit ook gezien.
Ik heb gisteren om 13h contact gehad met ID-ware met de mededeling dat wij een doelgroepenbericht zouden sturen. Dit doen we vaker (ook met Citrix destijds).
Toen kwam dit aan de orde. ID-ware vindt niet dat er persoonsgegevens bij de TK gelekt zijn. Ik heb toen aangegeven dat ID-ware dit via hun kanalen moet adresseren. Klaarblijkelijk zijn ze zelfstandig gaan communiceren.
Ik kom nog terug op je vraag.
07:24
8
Piket BZK gebeld. De piketmdw overlegt intern.


vodafone NL
22:13
Coördinatie ID-Ware
overlegt inte za 8 okt.
Heb aangegeven dat er al goede woordvoerings-/ commlijnen zijn.
Wordt vervolgd. 07:54
Terugkoppeling na gesprek met piket BZK: woordvoering pakt het op (samen met de andere departementen). Ik verwacht niet dat er publiekelijk wordt gereageerd, maar dat het maandag inhoudelijk wordt opgepakt. 08:47
5.1.2.e
5.1.2.e
Dank voor het uitzoeken en deze terugkoppeling
5.1.2.e
Terugkoppeling na gesprek met piket BZK: woordvoering pakt h...
8
Wordt woordvoering TK ook


vodafone NL
22:13
Coördinatie ID-Ware
betrokken?
za 8 okt.
5.1.2.e
En EK:)
08:49
5.1.2.e
5.1.2.e
Wordt woordvoering TK ook betrokken?
5.1.2.e
En woordvoering EK
08:49
5.1.2.e
Het is dezelfde groep woordvoerders die ook betrokken was bij de brief.
Maar zoals we weten: "assumptions are ...." Ik check het bij onze woordvoering of EK en TK zijn betrokken.
5.1.2.e
08:53
5.1.2.e
5.1.2.e
Het is dezelfde groep
8


vodafone NL
22:13
Coördinatie ID-Ware
5.1.2.e
za 8 okt.
Het is dezelfde groep woordvoerders die ook betrokk...
5.1.2.e
Fijn dank je
08:54
5.1.2.e
Er is een aparte signalgroep voor Woordvoering. Daar zitten naast BZK en J&V ook EK/TK bij.
5.1.2.e
09:02
5.1.2.e
Even voor alle helderheid: TK heeft niet met ID ware gecommuniceerd. Niet over tijdstip of inhoud van externe communicatie. Evenmin over onze eigen onderzoeksbevindingen. Dit omdat de coördinatie van dit alles bij het NCSC ligt. Saillant is wel, dat 5.1.2.f van ID ware aan mijn team de link op het
8


vodafone NL
22:13
Coördinatie ID-Ware
5.1.2.e
Even voor al. za 8 okt. .ıeid: TK heeft niet met ID ware gecommuniceerd. Niet over tijdstip of inhoud van externe communicatie. Evenmin over onze eigen onderzoeksbevindingen. Dit omdat de coördinatie van dit alles bij het NCSC ligt. Saillant is wel, dat 5.1.2.f van ID ware aan mijn team de link op het darkweb gaf waar we de gelekte info van onze pashouders aantroffen. Ze zeiden: je moet daar eens gaan kijken. Zo kwamen wij erachter. Ofwel: dat moet men daar ook hebben gezien.
09:54
Nog iets over op- of afschalen. Wij zullen ook een discussie moeten hebben over de
5.1.2.b
8

vodafone NL 22:13

Coördinatie ID-Ware

Nog iets ove za 8 okt. fschalen.
Wij zullen ook een discussie moeten hebben over de toekomst. 5.1.2.b

5.1.2.e

00

5.1.2.e

Aanvulling: wij hebben ook niet met ID-ware gecommuniceerd over bevindingen TK richting ID-ware.

Waarschijnlijk heeft ID-ware de link vernomen van de actor of de IR-partij die ze hadden

8

vodafone NL 22:14

Coördinatie ID-Ware

za 8 okt.

Waarschijnlij[redacted]-ware de link vernomen van de actor of de IR-partij die ze hadden ingehuurd. De actor heeft een site op het Darkweb en ID-ware schijnt te zijn benaderd door de actor volgens artikel nu.nl 10:08

5.1.2.e

5.1.2.e [redacted]

All, ik verlaat deze signal groep aangezien ik mijn werkzaamheden overgedragen heb aan 5.1.2.e . Hij is vanuit NCSC het eerste aanspreekpunt voor dit event.

5.1.2.e

12:44

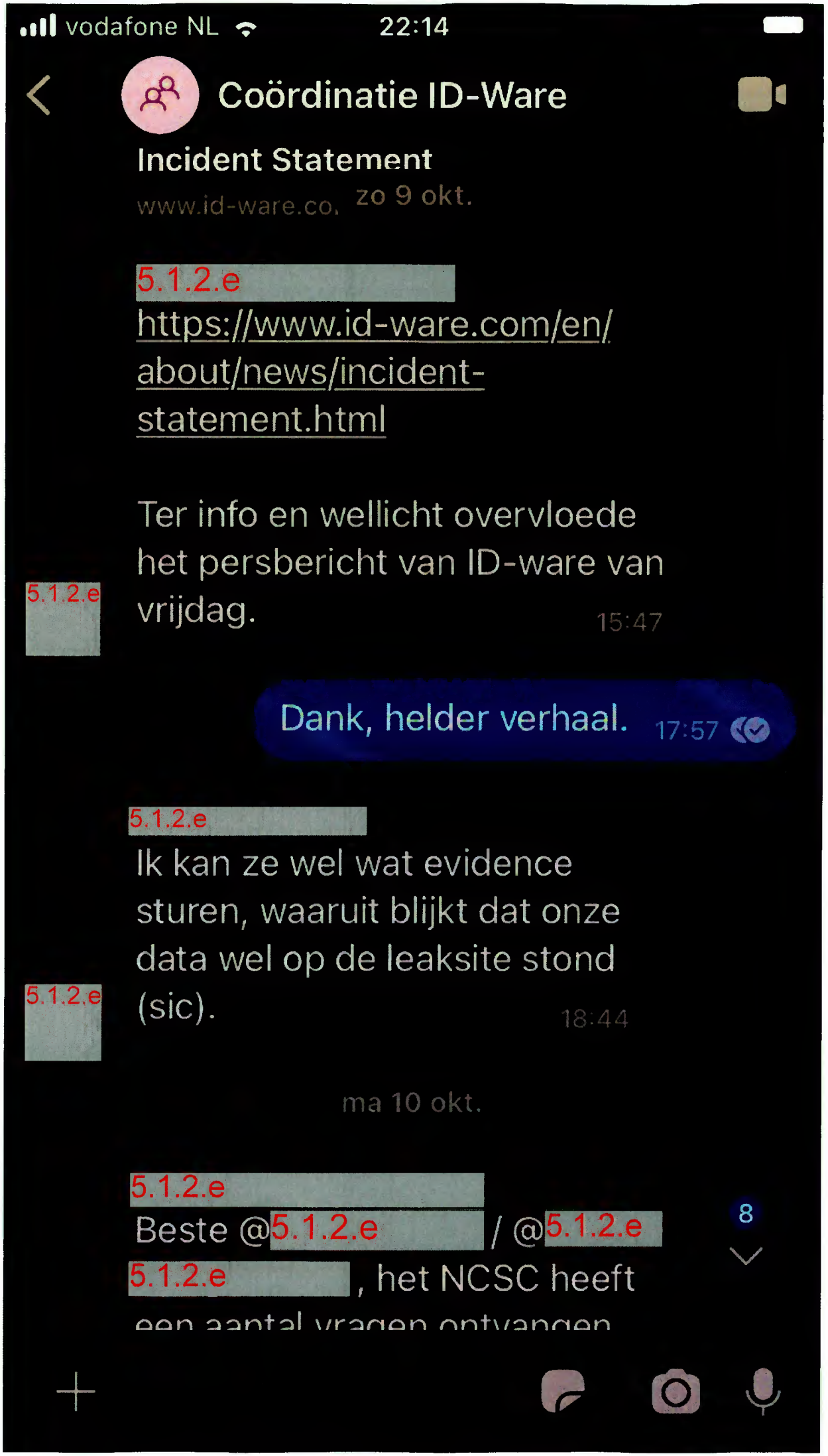
5.1.2.e [redacted] heeft de groep verlaten.

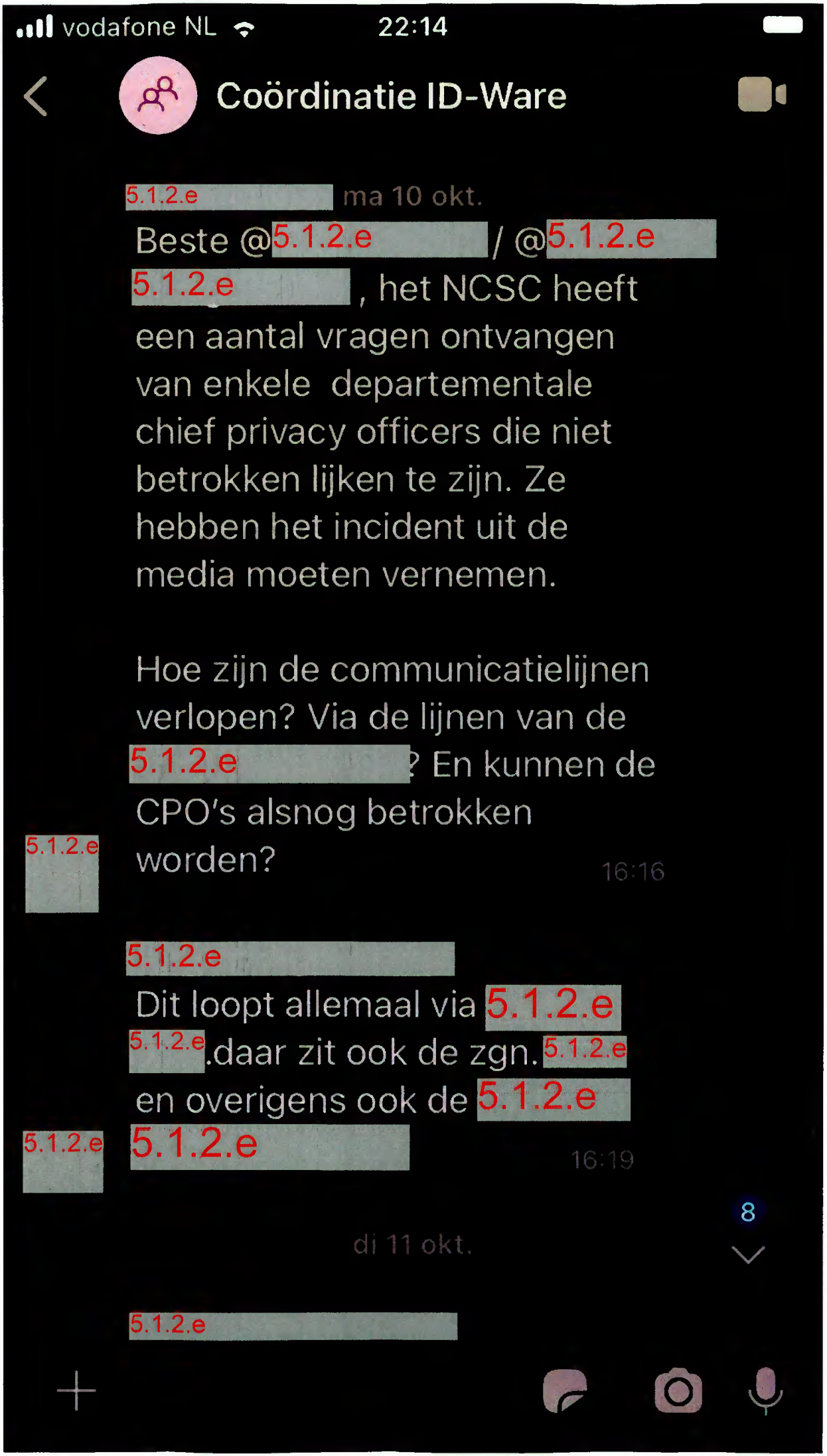
zo 9 okt.

8

Incident Statement

www.id-ware.com


vodafone NL
22:14
Coördinatie ID-Ware
Incident Statement
www.id-ware.co.
zo 9 okt.
5.1.2.e
https://www.id-ware.com/en/about/news/incident-statement.html
Ter info en wellicht overvloede het persbericht van ID-ware van vrijdag.
15:47
Dank, helder verhaal.
17:57
5.1.2.e
Ik kan ze wel wat evidence sturen, waaruit blijkt dat onze data wel op de leaksite stond (sic).
18:44
ma 10 okt.
5.1.2.e
Beste @5.1.2.e / @5.1.2.e
5.1.2.e , het NCSC heeft
een aantal vragen ontvangen
8


vodafone NL
22:14
Coördinatie ID-Ware
5.1.2.e
ma 10 okt.
Beste @5.1.2.e / @5.1.2.e
5.1.2.e , het NCSC heeft een aantal vragen ontvangen van enkele departementale chief privacy officers die niet betrokken lijken te zijn. Ze hebben het incident uit de media moeten vernemen.
Hoe zijn de communicatielijnen verlopen? Via de lijnen van de 5.1.2.e ? En kunnen de CPO's alsnog betrokken worden?
16:16
5.1.2.e
Dit loopt allemaal via 5.1.2.e
5.1.2.e .daar zit ook de zgn. 5.1.2.e en overigens ook de 5.1.2.e
5.1.2.e
16:19
8
di 11 okt.
5.1.2.e


vodafone NL
22:14
Coördinatie ID-Ware
5.1.2.e
di 11 okt.
Allen, vanaf vandaag neemt
5.1.2.e
5.1.2.e het stokje over als coördinator.
5.1.2.e leidt ook (sinds vorige week) het technisch team dat nog onderzoek doet naar de dataset.
Nu de onmiddellijke operationele coördinatie niet meer nodig is, zal ik vandaag aan 5.1.2.e vragen of hij ook in deze groep moet komen. 06:25
5.1.2.e
Ok, dank voor de support, 5.1.2.e
09:01
5.1.2.e
Goedemorgen,
Wij hebben verschillende
vragen: we zijn onder andere
8


vodafone NL
22:14
Coördinatie ID-Ware
5.1.2.e
di 11 okt.
Goedemorgen,
Wij hebben verschillende vragen: we zijn onder andere benieuwd of er gister nog contact is geweest nav ID ware uitingen in de media? Leidt dat nog tot aanvullende communicatie? Ook horen we graag of er al meer bekend is over aantallen gegevens die weg zijn genomen.
We overleggen ook graag over vervolg van dit traject richting ID-ware en evaluatie.
Is het een idee dat we hiervoor bij elkaar komen?
5.1.2.e
10:21
Ha 5.1.2.e
8
- er is zaterdag wat overleg


vodafone NL
22:14
Coördinatie ID-Ware
di 11 okt.
Ha 5.1.2.e
- er is zaterdag wat overleg geweest met woordvoering. Het statement van ID-ware is niet onjuist, en is ook niet in tegenspraak met de brief en de communicatie naar de pashouders (maar ook niet compleet).
D66 gaat een mondelinge vraag stellen tijdens het vragenuurtje. De stass heeft hiervoor de nodige facts en Q&A.
- voorzover mij bekend is van 75.000 bestanden en/of 221 Gb vastgesteld dat ze zijn gelekt. Misschien heeft NCSC nog een update?
8
- de vraag over het traject


vodafone NL
22:14
Coördinatie ID-Ware
- voor di 11 okt. bekend is van 75.000 bestanden en/of 221 Gb vastgesteld dat ze zijn gelekt. Misschien heeft NCSC nog een update?
- de vraag over het traject richting ID-ware spe...
Meer lezen
10:39
5.1.2.e
Het statement van ID ware is wel onjuist. Zij stellen dat er geen bewijs is dat data van parlementsleden is gelekt. Dat bewijs is er wel, nl de logbestanden.
11:04
5.1.2.e
5.1.2.e
Jij
Ha 5.1.2.e ,
8
Dank voor de reactie.


vodafone NL
22:14
Coördinatie ID-Ware
Jij
di 11 okt.
Ha 5.1.2.e ,
Dank voor de reactie.
Ik sluit mij aan bij 5.1.2.e , het statement van ID ware was in mijn ogen Onjuist.
Ik ben benieuwd hoe dit in de beantwoording van mondelinge vragen terug komt, met name als het om Kamerleden gaat hoop ik dat antwoorden afgestemd zijn met Tweede Kamer communicatie. Ik heb dit intern ook nagevraagd.
11:33
5.1.2.e
5.1.2.e
Jij
Ha 5.1.2.e ,
8
Wij hebben wel een update,


vodafone NL
22:14
Coördinatie ID-Ware
Jij
di 11 okt.
Ha 5.1.2.e ,
Wij hebben wel een update, maar het lijkt me goed om (virtueel) af te spreken.
NCSC doet momenteel onderzoek naar de echtheid van de dataset en de inhoud met het oog op een beeld voor RO+vitaal.
We verwachten do/vr meer info te hebben.
5.1.2.e
Inmiddels hebben we de gelekte data binnen.
11:33
5.1.2.e
Voor mij begint dit alles via Signal een beetje onoverzichtelijk te worden. Ik zou graag in één keer goed
8


vodafone NL
22:14
Coördinatie ID-Ware
5.1.2.e
di 11 okt.
Voor mij beg... ...es via Signal een beetje onoverzichtelijk te worden. Ik zou graag in één keer goed horen wat nu wel en niet waar is..
11:35
5.1.2.e
Precies. Is het handig om alvast een afspraak te maken? Bijv. donderdag om 12:00? Ik kan jullie wel uitnodiging + webex sturen.
11:38
5.1.2.e
Ik kan pas rond 14.30
11:40
5.1.2.e
ok, ik zal het aan ons secretariaat vragen om iets in te plannen.
11:41
8
5.1.2.e
Mij lukt het waarschijnlijk niet

vodafone NL 22:14

Coördinatie ID-Ware

5.1.2.e

ma 11 okt.

Mij lukt het waarschijnlijk niet om aan te sluiten. @5.1.2.e wil jij dit aub naar mij toe terugkoppelen? 11:42

5.1.2.e

5.1.2.e

Vraag ID-Ware komt niet in vragenuurtje 12:42

wo 12 okt.

5.1.2.e

5.1.2.e

Vervelend, 5.1.2.e. Beterschap.

Ik stel voor dat we volgende week een afspraak organiseren. Dan is ons technisch onderzoek ook klaar (denk ik). 08:40

8

5.1.2.e


vodafone NL
22:14
Coördinatie ID-Ware
5.1.2.e
Vervelend, 5.1.2.e wo 12 okt. schap.
Ik stel voor dat we volgende week een afspraak organiseren. Dan is ons technisch onderzoek ook klaar (denk ik).
08:40
5.1.2.e
5.1.2.e
Oh sterkte en beterschap 5.1.2.e
10:15
5.1.2.e
5.1.2.e
Beterschap!
10:15
za 15 okt.
5.1.2.e
https://www.ad.nl/eindhoven/high-tech-campus-slachtoffer-van-hack-bij-it-bedrijf-fotos-van-duizenden-werknemers-belanden-op-dark-web~ac1f90d4/
7
Is premium artikel dus wellicht

vodafone NL 22:15

Coördinatie ID-Ware

5.1.2.e

hack bij ID-ware 10:46

za 15 okt.

5.1.2.e

PDF signal-2022...-105552.pdf
52 KB

Met de groeten van abonnee

5.1.2.e

5.1.2.e 10:59

5.1.2.e

Dank voor de info. Ik heb de url doorgezet naar de cert-box van het NCSC.

NCSC is niet meer intern opgeschaald voor deze casus, maar neemt deze media-aandacht wel in het beeld op. Vanzelfsprekend wordt er gepast gehandeld indien dit nodig is.

5.1.2.e 11:54

do 20 okt.

4

5.1.2.e


vodafone NL
22:15
Coördinatie ID-Ware
5.1.2.e
do 20 okt.
Gegevens [redacted] studenten TU Eindhoven en Hogeschool Utrecht gelekt bij hack https://www.rtlnieuws.nl/economie/artikel/5341242/datalek-tu-eindhoven-hogeschool-utrecht-ransomware-id-ware-pashouders
16:20
5.1.2.e
Het nieuws was zojuist ook op BNR. Deze gegevens hebben we ook in de dataset gezien en twee weken geleden ook Surfcert ingelicht.
16:26
5.1.2.e
Het wordt wel een steeds grotere 'vlek'
16:27
5.1.2.e
"Een woordvoerder van de universiteit laat weten dat er
1

vodafone NL 22:15

Coördinatie ID-Ware

5.1.2.e grotere vlek 16:27

do 20 okt.

5.1.2.e

"Een woordvoerder van de universiteit laat weten dat er geen direct misbruik gemaakt kan worden gemaakt van de gegevens. Kwaadwillenden kunnen volgens hem geen toegang krijgen tot data of gebouwen van de TU Eindhoven."

Opvallend dat de woordvoerder zo stellig is terwijl ik nog niet durf te zeggen van welke klanten de gelekte geheime pas-sleutels zijn, er zijn in ieder wachtwoorden gelekt die tenzij ze gewijzigd zijn konden inloggen op ID-ware systemen met klanten data en andere plaatsen waar hetzelfde

5.1.2.e wachtwoord is gebruikt 17:15

Oplegger Mondelinge Vraag

Onderwerp: het hack van rijkspassen
Bewindspersoon: Staatssecretaris van Koninkrijksrelaties en Digitalisering
Naam dossierhouder: 5.1.2.e
Telefoonnummer en e-mailadres dossierhouder: 5.1.2.e

Mondelinge vraag van het lid:

Aanpassen dit voorbeeld: - het lid **Dekker-Abdulaziz** (D66) aan de staatssecretaris voor Koninkrijksrelaties en Digitalisering over het hack bij ID-ware/de rijkspas (nav Kamerbrief op vrijdag 7 oktober; opgepakt door verschillende media)

Kern van het mediabericht	**Per brief heeft u de Kamer op vrijdag 7 juli geïnformeerd over de hack op ID-ware, een leverancier in het kader van de uitgifte van Rijkspassen. Deze worden gebruikt door het Rijk, Eerste en Tweede Kamer. Er zijn bij de aanval persoonsgegevens van bijna 3500 medewerkers (naam, rijkspasnummer en paraaf) uitgelekt. Er zijn voor zover nu bekend geen gegevens van Eerste of Tweede Kamerleden gelekt, ondanks verwarring daarover in mediaberichtgeving.**
Kernboodschap van de bewindspersoon	Het is betreurenswaardig dat de gegevens zijn gelekt. Er wordt momenteel nog onderzoek uitgevoerd door onder andere het NCSC en de politie. Het lek zal voor de gebruiker naar verwachting een beperkte impact hebben. We zullen de situatie niettemin nauwgezet monitoren zowel voor de medewerkers als op de systemen van Rijkspasbeheer, de Eerste Kamer en Tweede Kamer. Indien daar aanleiding toe is, zullen updates volgen.
Argumentatie	• Het is betreurenswaardig dat de gegevens gelekt zijn. • Voor nu zijn en worden de betrokken organisaties en personen geinformeerd. • Voor zover nu bekend, zitten er geen gevens van Eerste en Tweede Kamerleden tussen. • We blijven de situatie monitoren, en acteren wanneer dat nodig blijft. • We verwachten dat de impact beperkt is. • Voor verdere feiten is het van belang dat de verschillende onderzoeken nu worden doorlopen. • Daar kan ik nu niet op vooruit lopen. • Wel zal ik de Kamer waar nodig nader informeren de komende periode.
Feiten en cijfers	• (Een uitgebreidere factsheet en tijdlijn is als bijlage bijgevoegd.) • Sommige media (Volkskrant, Telegraaf) melden dat er gegevens van Kamerleden op straat liggen. Dit is voor zover nu bekend niet het geval, en is zo ook niet in de brief aan de Kamer vermeld. Ook ID-ware zelf ontkent dit. • Het incident vond plaats van 17 op 18 september. • Op 21 september vond het eerste contact plaats tussen CISO Tweede Kamer en CISO Rijk. • De weken daarna is er met regelmaat contact geweest. • De gegevens van ongeveer 3500 personen zijn gelekt. • Nader onderzoek loopt nog en zal minimaal nog een aantal weken of maanden in beslag nemen. • Er is nog niet vernomen of AP een onderzoek gaat starten.
Politieke afspraken (relevante passages regeerakkoord, verkiezingsprogramma's,	Cybersecurity is een de punten waar in het regeerakkoord op wordt ingegaan. Op 10 oktober heeft de Kamer de Nederlandse Cyber Security Strategie (NLCS) ontvangen, waarin de kabinetsinzet op cybersecurity wordt ingezet. Deze bevat ook acties voor de (rijks)overheid.

moties en/of toezeggingen)	
Overig	

31

Ministerie van Justitie en Veiligheid

Berichtgeving hack toegangspasjes Kamer
Berichtgeving van de Volkskrant wordt overgenomen door verschillende grotere nieuwssites.

- Data Kamerleden gelekt door hack bij IT-bedrijf: gegevens toegangspassen online (volkskrant.nl)
- Gegevens toegangspassen Kamerleden op criminele site na hack bij IT-bedrijf | Binnenland | Telegraaf.nl
- Gegevens bijna 3.500 toegangspassen overheidsinstellingen gelekt - NRC
- Bedrijf in toegangspasjes gehackt: gegevens kamerleden liggen op straat | Tech | NU.nl
- Data toegangspassen Tweede Kamerleden op straat na hack bij IT-bedrijf | Tech | AD.nl
- 'Data Kamerleden gelekt door hack bij IT-bedrijf' | BNR Nieuwsradio
- Persoonsgegevens Kamerleden gestolen door datalek bij IT-bedrijf | Noordhollands Dagblad
- GeenStijl: Data toegangspasjes Tweede Kamer geHACKT

En door vakmedia:

- Hack bij ID-ware treft passen van Eerste en Tweede Kamer | Dutch IT-channel (dutchitchannel.nl)
- Groot datalek bij Nederlandse overheid - AG Connect
- Privédata duizenden rijksambtenaren gelekt na inbraak op servers ID-ware - Security.NL
- Toegangspassen politici en ambtenaren gehackt | Computable.nl
- Gegevens toegangspassen Tweede Kamer gehackt - BeveiligingNieuws

Social media
Op social media is het nieuws nog niet erg groot opgepikt. Het nieuws wordt vooral gedeeld door journalisten. Discussie of specifieke vragen/informatiebehoefte zijn nog niet te zien. Een enkeling maakt een opmerking over de overheid i.c.m. ict, of een algemene waarschuwing tegen digitalisering:

- Pieter v Vollenhoven op Twitter: "Data Kamerleden gelekt door hack bij IT-bedrijf: gegevens toegangspassen online! Over onze kwetsbaarheid gesproken!!! Wij willen óók nog zelfrijdende auto's....waar gaan die naar toe als zij gehackt worden? https://t.co/IQa8c4Adxc" / Twitter
- Huib Modderkolk op Twitter: "Nieuws: door een hack bij it-bedrijf ID-ware zijn de data van honderden klanten gelekt, waaronder oa de gegevens van toegangspassen van Tweede Kamerleden. Parlement wordt vanmiddag geïnformeerd. https://t.co/rNwPD1x1A2" / Twitter
- Remko Theulings op Twitter: "Data Kamerleden gelekt door hack bij IT-bedrijf: gegevens toegangspassen online https://t.co/bJlYUxbZec" / Twitter
- Mike Muller op Twitter: "Gegevens toegangspassen Kamerleden op criminele site na hack bij IT-bedrijf https://t.co/CNi8v0TF4J via @Telegraaf" / Twitter