To: 5.1.2e)[5.1.2e @minvws.nl]; 5.1.2e)[5.1.2e @minvws.nl]
From: 5 5.1.2e)
Sent: Mon 1/25/2021 1:38:27 PM
Subject: RE: spoed datalek HP Zone
Received: Mon 1/25/2021 1:38:28 PM

Dat is wat mij tot nu toe bekend is. Er zijn twee medewerkers aangehouden, die geen link met elkaar hebben overigens, voor het aanbieden van screenshots met persoonsgegevens en bijbehorende contacten. Het zou gaan om mensen die in de getuigenbescherming zitten. De dataset die is gedownload staat hier los van.

En ik heb net, na telefonisch contact met Ron, wat vervolgvragen gesteld over die SQL-injectie. En de suggestie van VPN en 2FA meegegeven.

Gr 5.1.2e

Van: 5.1.2e) < 5.1.2e @minvws.nl>
Verzonden: maandag 25 januari 2021 14:31
Aan: 5.1.2e) < 5.1.2e @minvws.nl>; 5. 5.1.2e) < 5.1.2e @minvws.nl>
Onderwerp: RE: spoed datalek HP Zone

Is de analyse dus dat het lek is uitgevoerd door een medewerker met toegang tot HP Zone?
Dat maakt het geen hack, maar vooral een datalek.

In verdere opvolging extra aandacht geven aan gebruik VPN en 2FA om remote access door gebruikers landelijke partners en eigen medewerkers goed af te schermen. Meen me te herinneren dat dat nog niet geregeld was

Van: 5.1.2e) < 5.1.2e @minvws.nl>
Verzonden: maandag 25 januari 2021 14:26
Aan: 5. 5.1.2e) < 5.1.2e @minvws.nl>
CC: 5.1.2e) < 5.1.2e @minvws.nl>
Onderwerp: RE: spoed datalek HP Zone

Bijzonder. Maar dank!

Van: 5. 5.1.2e) < 5.1.2e @minvws.nl>
Verzonden: maandag 25 januari 2021 14:24
Aan: 5.1.2e) < 5.1.2e @minvws.nl>
CC: 5.1.2e) < 5.1.2e @minvws.nl>
Onderwerp: RE: spoed datalek HP Zone

Ik heb begrepen dat er drie mogelijke oorzaken waren, waar SQL injectie er een van is (en misbruik van BI een derde). Maar er is aangetoond dat die export daadwerkelijk heeft plaatsgevonden. Ik heb niet gehoord dat die SQL-injectie daadwerkelijk is geconstateerd.

Gr. 5.1.2e

Van: 5.1.2e) < 5.1.2e @minvws.nl>
Verzonden: maandag 25 januari 2021 14:18
Aan: 5. 5.1.2e) < 5.1.2e @minvws.nl>
CC: 5.1.2e) < 5.1.2e @minvws.nl>
Onderwerp: RE: spoed datalek HP Zone

Er was toch ook een sql injectie?

Gr

5.1.2e

Van: 5. 5.1.2e) < 5.1.2e @minvws.nl>
Verzonden: maandag 25 januari 2021 14:13
Aan: 5.1.2e) < 5.1.2e @minvws.nl>
CC: 5.1.2e) < 5.1.2e @minvws.nl>; 5.1 5.1.2e) < 5.1.2e @minvws.nl>; 5.1.2e . (5.1.2e) < 5.1.2e @minvws.nl>; 5.1.2(5.1.2e) < 5.1.2e @minvws.nl>
Onderwerp: RE: spoed datalek HP Zone

Beste 5.1.2e

Zojuist heb ik overleg gehad met GGD/GHOR, een informatiebeveiligingsexpert van VWS en mensen die hebben meegewerkt aan de Risicoanalyse. Dat levert de volgende korte antwoorden:

5.1.2i Concept

5.1.2e

IK verwacht hier morgen in vragenuur TK ook wel vragen over.

Met vriendelijke groet,
5.1.2e

Van: 5.1.2e) < 5.1.2e @minvws.nl>
Verzonden: maandag 25 januari 2021 12:52
Aan: 5. 5.1.2e) < 5.1.2e @minvws.nl>; 5.1.2e) < 5.1.2e @minvws.nl>
CC: 5.1.2e) < 5.1.2e @minvws.nl>; 5.1 5.1.2e) < 5.1.2e @minvws.nl>
Onderwerp: spoed datalek HP Zone
Urgentie: Hoog

Beste 5.1.2e

Mede namens 5.1.2e verzoek ik jou als voorzitter van de regiegroep ons met spoed te rapporteren over het datalek bij GGDen (ik begrijp: gegevens van positief geteste personen en hun contacten aangeboden op darkweb én te koop aanbieden van persoonsgegevens door mw van Teleperformance, deze mail gaat over het eerstgenoemde).
Mag ik de rapportage ajb om 14 uur ontvangen ajb?

In hoeverre is dit datalek ook te relateren aan de risico-analyse die heeft plaatsgevonden over de ICT van GGDen?
Kwam dit soort lekken daarin ook naar voren?

Zo ja, wat was de beheersmaatregel en is men ook al begonnen om die maatregel toe te passen?

Zo nee, hoe denk je dat dit komt? waarom is dit denk je niet in de risico analyse naar voren gekomen?

Wat gaan we/GGDen hier aan doen om te zorgen dat het niet meer voor komt? Hoe helpt VWS de GGDen? Wanneer is het geregeld/klaar?

Kunnen we de gegevens wegkrijgen van darkweb?

Geeft het bovenstaande aanleiding tot ee nieuwe prioriteitstelling in het aanpakken van de beheersmaatregelen?

IK verwacht hier morgen in vragenuur TK ook wel vragen over.

Met dank en groet,

5.1.2e

5.1.2e 5.1.2e 5.1.2e

Ministerie van VWS
Telefoonnummer secretariaat: 070 5.1.2e