To: 5.1.2e)[5.1.2e @minvws.nl]; 5.1.2e)[5.1.2e @minvws.nl]
Cc: 5.1.2e]; 5.1.2e)[5.1.2e @minvws.nl]
From: 5.1.2e)
Sent: Tue 9/29/2020 8:36:19 AM
Subject: Beveiligingsrapportages, vandaag publiceren
Received: Tue 9/29/2020 8:36:19 AM
20200928 Duidingsrapportage Coronamelder.pdf
Bijlage I - Codereview Radically Open Security.pdf
Bijlage K - Rapportage Penetratietest.pdf

Dag 5.1.2e

Hierbij de rapporten die vandaag gepubliceerd zouden worden met bijbehorende duidingsrapportage. Met 5.1.2e is eerder afgesproken om te publiceren en mijn dringende advies is dat ook te doen 5.1.2a . Met de TK is eerder besprokend at we bij voortduring openbaar maken. Ik zie ook geen grote risico's. Onderstaand de meest in het oog springende bevindingen en onze reactie. Indien toch TK geïnformeerd moet dan toch maar vandaag zonder beleidsreactie zou ik zeggen met reactie in volgende brief.

Onderzoek	**Bevinding**	**Reactie**
ROS	De GGD Ghor gebruikt een externe partij om veilig inloggen voor medewerkers te organiseren. ROS kende het afsprakenstelsel daarom heen niet	De leverancier maakte voldoende afspraken met GGD GHOR om te waarborgen dat sprake is van een voldoende veilig proces. Aanpassing niet nodig. ROS kende die afspraken niet
ROS	GGD medewerker kan zien of sleutels succesvol zijn geupload	Wordt verwijderd bij landelijke introductie. Geen groot risico (anders dan dat drang kan worden ervaren door gebruiker)
NFIR	De host ondersteunt de onveilige TLS-versies 1.0 of 1.1. Deze protocollen zijn sinds maart 2020 end-of-life en worden daarom niet meer ondersteund door de meest gebruikte browsers.	KPN biedt dit aan al haar klanten aan en kan dat niet voor CoronaMelder alleen aanpassen. Daarom is voor CoronaMelder een extra versleuteling van het dataverkeer toegevoegd waardoor dit risico is weggenomen.

Gr

5.1.2e