To: 5.1.2e)[5.1.2e @minvws.nl]
Cc: 5.1.2e [5.1.2e]; 5.1.2e [5.1.2e @cwi.nl]; 5.1.2e [5.1.2e @ 5.1.2e 5.1.2e)[5.1.2e @minvws.nl]; 5.1.2e)[5.1.2e @minvws.nl]; 5.1.2e [5.1.2e @cs.ru.nl]; 5.1.2e 5.1.2e [5.1.2e]; 5.1.2e [5.1.2e @publicmatters.nl]
From: 5.1.2e .
Sent: Wed 9/30/2020 7:39:17 PM
Subject: Re: Short call
Received: Wed 9/30/2020 7:39:21 PM

5.1.2e ontzettend bedankt voor je snelle en zeer gedetailleerde toelichting op alles, zwoel qua inhoudelijk en proces. Je bent inderdaad leeggelopen zie ik. Super uitgelegd, zelfs voor de wat minder technisch aangelegden.

Zoals wij vandaag al bespraken zijn velen, net als wij zelf, gisteren door dat VK-artikel vooral geschrokken en teleurgesteld door de uiteindelijke insteek en bewoordingen van de kop en Van de tekst in het eerste deel van het artikel. Dit hadden wij Zelf, als geïnterviewden, niet eens gezien. Zoals we beiden al tweetten vandaag, en zoals 5.1.2e erecht opmerkt, we moeten in nauwe samenwerking en vertrouwen snel doorpakken om de huidige zorgwekkende tweede golf het hoofd te gaan bieden.

Nogmaals dank,

5.1.2e

Op 30 sep. 2020 om 21:20 heeft 5.1.2e) < 5.1.2e @minvws.nl> het volgende geschreven:

Dank 5.1.2e

Voor de anderen: wij houden nooit bewust iets achter. Mensen zijn uitgeput en blijven proberen maximaal te presteren. Laten we daar van blijven uitgaan. We hebben samen een maatschappelijke uitdaging het hoofd te bieden. Ik ben trots op iedereen die hier aan werkt. Laten we iedereen heel houden.

Met vriendelijke groet,

5.1.2e
5.1.2e

Ministerie van Volksgezondheid, Welzijn en Sport

Postbus 20350 | 2500 EJ | Den Haag
Managementassistente: 5.1.2e | 5.1.2e @minvws.nl | 5.1.2e

T 5.1.2e
5.1.2e @minvws.nl

Van: 5.1.2e < 5.1.2e >
Verzonden: woensdag 30 september 2020 21:08
Aan: 5.1.2e < 5.1.2e @cwi.nl>
CC: 5.1.2e . < 5.1.2e @umcutrecht.nl>; 5.1.2e < 5.1.2e @ 5.1.2e 5.1.2e) < 5.1.2e @minvws.nl>; 5.1.2e) < 5.1.2e @minvws.nl>; 5.1.2e <5.1.2e @cs.ru.nl>; 5.1.2e < 5.1.2e >; 5.1.2e < 5.1.2e @publicmatters.nl>; 5.1.2e) < 5.1.2e @minvws.nl>
Onderwerp: Re: Short call

Beste 5.1.2e en anderen,

Dank voor je mail ik reageer tussen de regels door, want dan weet ik zeker dat ik niets mis.

Op 30-09-2020 om 19:22 schreef 5.1.2e:

> Ik vrees dat het wat moeilijk is om op stel en sprong zo'n gesprek te regelen.
> Daarnaast zou ik dan ook 5.1.2e willen aanschakelen (cc:).

Helemaal prima. Ik wil namelijk heel duidelijk en zo breed mogelijk communiceren dat ik niemand iets heb onthouden, dat 5.1.2e op geen enkel moment zoiets gevraagd is en dat er geen spelletjes zijn gespeeld. Iedereen op het team weet dat dit een complex project is waar je veel hobbels gaat tegenkomen. Wat de feitelijke gang van zaken is geweest is het volgende:

1. Toen ik het plan maakt om breed en diep te testen met verschillende bedrijven was mijn doel: veel bevindingen krijgen, mooie software krijgen en vooral nergens voor wegduiken. Juist meerdere bedrijven geven immers een grotere kans dat overlappende bevindingen worden gedaan. Zo dek je alles af. De partijen die zijn gekozen, zijn in mijn ogen de beste. Secura/ROS voor de code. NFIR voor de pentest. In aanloop naar de start van testen ontstond zelfs paniek bij bedrijven "wat als mijn concurrent iets vindt wat ik zou moeten vinden?". Dus hebben alle drie de bedrijven om niet meer gedaan dan gevraagd. Had ik de weg van de ministe weerstand gekozen dan had ik de pentestpartij van Infectieradar.nl wel gekozen. Dan weet je zeker dat de OWASP TOP-10 niet wordt bevonden.
2. De broncodetesten heb ik bewust vanaf de publieke repo laten plaatsvinden, zodat iedereen kon meekijken. De bedrijven geen sturing gehad om ze ergens bij weg te houden. Juist niet.
3. Er is de harde afspraak gemaakt: hoge bevindingen meldt je onverwijld, zodat we er meteen mee aan de slag konden. Dat is ook zo gebeurd. Dus daarom kon ik ook zeggen dat er geen showstoppers waren (op de inhoud kom ik zo terug). Er was op geen enkel moment een reden tot zorg. Anders verbind ik - gelet op het afbreuk risico mijn naam er niet aan.
4. Op 28 augustus 2020 moest er een brief naar de kamer. Secura was klaar dus dat rapport is bijgevoegd. NFIR nog niet dus heb ik een managementsamenvatting gevraagd. Die heb ik ook gekregen. Alleen ROS kon niet leveren door een bug in hun XML-systeem. We hebben gewacht, maar op vrijdag 18 uur moest de brief er toch echt uit. Het rapport ROS zat er niet bij. Context: ik was die week op vakantie in Frankrijk - wel gewerkt niet op ministerie.
5. De reden dat de onderzoeken nog niet af waren, is dat wij de tijd maximaal benut hebben om te testen, hertesten en voor code audits zoveel mogelijk alle changes te laten beoordelen. Afronden van de opdracht betekent een nieuw inkoopproces starten. Ik heb gekozen voor maximaal testen.
6. Om 18:42 kwam het rapport ROS en kon het niet meer met de kamerbrief mee. Er is geen titel het dan te sturen. Dan is normaal dat je het met de volgende kamerbrief stuurt en die komt pas in oktober. Zo werkt dit systeem nu eenmaal, maar er is dus niets achtergehouden. Er is geen trucendoos toegepast. Dus toen de Volkskrant erom vroeg hebben we gezocht naar een manier om ze zo goed mogelijk te bedienen. Dat was de route via github. Om dat te kunnen en om niet-techneuten wel te duiden moest daarvoor wel een duiding komen. Dat zijn de toevoegingen met bevindingen, oplossingen, maatregelen en ook de risicoinschatting.

Dan het proces met de Volkskrant

1. Er was aandacht voor de bevinding met de hoge classificering 'The Identity Hub'. Alleen toen de journalist doorkreeg dat dit niet VWS, maar onder gemeenten viel (en dus BZK) was de interesse weg.
2. Toen kwam het tweede punt. Daarvan is heel duidelijk gesteld - bij herhaling - dat dit geen fout betrof, maar functionaliteit voor het doen van de testen. De persoon zei dat te begrijpen, maar het werd opeens toch een ding.
3. Vervolgens werd ik geconfronteerd met de stelling dat ROS wel eerder zou hebben gemaild. Ik heb de communicatie met ROS overlegd waaruit de tijdlijn bleek. Ook vanuit ROS is exact hetzelfde

feitencomplex aangediend, omdat dit nu eenmaal de waarheid was. De Volkskrant persisteerde in de passage over niet informeren kamer en zij wisten bij het live gaan al dat de werkelijkheid anders was.
4. Vandaag op Twitter maak ik op dat men nu anders denkt, maar het beeld is geschapen.
5. Uiteraard heb ik aangeboden door alle documenten te gaan, ik heb aangeboden de juiste mensen erbij te halen en iedere bevinding te bespreken. Hiervoor was geen interesse. De journalist in kwestie was zelf verantwoordelijk voor de digitalisering van de Volskrant en was bekend met het proces van bugs gaf hij aan.

Wat ons in de commissie bevreemd is dat we dit document wel een paar keer hebben opgevraagd, maar niet gekregen.

Bij mijn weten is mij een keer de vraag voorgelegd vanuit de commissie of de beveiligingsonderzoeken er waren. Die waren er niet en dat heb ik geantwoord. Meer dan dat weet ik simpel weg niet. Voor mij is niet duidelijk waarom ik iets niet zou geven. Ik hou niets achter.

Uiteindelijk staan er dus wat pikante zaken in (met name het inbouwen van die achterdeur om te kijken of TEKs werden ge-upload), zodat we de indruk hebben dat het document bij ons is weggehouden.

Nee hoor er staat niets pikants in. In de testfase weten we veel dingen niet. Ik geef een paar vragen:

1. Snappen mensen de interface wel?
2. Lopen mensen vast of ging het proces wel goed?
3. Twijfels bij de medewerker of het systeem werkt?
4. Trekt de backend de load echt zoals we hadden verwacht?
5. Wordt de link tussen sleutels en code echt goed gelegd?

Een paar zaken die in de praktijk spelen. Vanuit de GGD kwam het verzoek om dat via een vinkje te kunnen zien (groen gelukt). Voor de testfase paste dat binnen de DPIA en was geen reden om in de weg te staan. Bij de livegang was altijd het idee het te verwijderen.

Laten we even de context schetsen van het proces. Iemand krijgt Corona. Vervolgens hang je ruim twee uur aan de lijn voor het bron- en contactonderzoek. Daar wordt de hemd van het lijf gevraagd. In dat traject van ondersteuning is het niet vreemd om tijdens de testfase die visuele feedback te hebben. Voor lancering zou dit al verwijderd worden. In de bijlage zie je de visuele confirmatie dat bijna drie dagen voor de Volkskrant bedacht om dit frame op ons los te laten de feature in de interne repo al was gewist. Kortom: er is niets verwijderd naar aanleiding van een bevinding of de dreiging van een artikel.

De bevinding van ROS op de openbare code is op zichzelf een terechte, want zonder sturing weten ze niet dat dit ging fout betreft. Precies zo wil ik ook dat onderzoek wordt gedaan.

Dan verder nog even: hoe werkt het verbergen van bevindingen met een bedrijf als Radically Open Security in een project waar alle externen vrij mogen praten in een open project vol met kritische volgers?

Hoe dit zo gelopen is, is dus een eerste vraag.

Zoals boven beschreven.

Een van de keren dat we dit bespraken was niet per mail, maar met jou in de commissievergadering, overigens.

En toen heb ik geen blad voor de mond genomen, mijn zorgen geuit en exact verteld wat ik wist.

Een tweede vraag is natuurlijk wat er met de belangrijkste bevindingen gedaan

wordt.

Dat staat exact beschreven in de duidingsrapportage met *alle* bevindingen die er tot nu toe zijn. Om maar direct te zijn over de ROS bevindingen:

1. De hoge bevinding van ROS is authenticatie bij de GGD. Zij kwalificeren een externe partij voor authenticatie als een hoog risico. Alleen zij kijken naar code niet naar procedures of feitelijkheden van de implementatie. De bevinding is doorgeleid naar GGD/GHOR. Zij geven met hun leverancier aan dat de oplossing weldegelijk bij de GGD draait en dat er afspraken zijn. Kloppen die? Ik ga het binnenkort onderzeken in het kader van app2. Overigens is het een interessante securityvraag of GGD/GHOR beter af zou zijn als zij zelf authenticatiemanagement zouden gaan optuigen.
2. De bevinding van het stuk in de Volkskrant is dus geen fout, is dus niets blijvends en is zeker niet het grote complot dat nu een beetje door ze wordt voorgespiegeld.
3. Er zijn een tweetal bevindingen die zijn doorgeleid naar Apple/Google. Die zijn niet opgepakt. Daarom hebben we daarvoor een tweetal CVE (Common Vulnerability Disclosures) gemaakt. Ze krijgen nummer CVE-2020-24721 & CVE-2020-24722 en zouden zeer binnenkort live komen. Ofwel: we doen niets in het geniep, maar juist meer open dan menig big tech bedrijf prettig vindt. Leuk detail: ik heb dit de Volkskrant voorgehouden voordat duidelijk werd dat men weinig goeds in de zin gehad. Dit is namelijk behoorlijk cool en open.
4. Wat er gebeurt met alle bevindingen staat in de duidingsrapportage en in deze Google Docs:

5.1.2h

Het proces van afweging is simpel:

1. Is het een ding dat we kunnen fixen? Doen!

2. Is het ondervangen door iets anders of kijken we er tegenaan bespreken en zo aftikken.

Mijn voorstel is om je dan uit te nodigen volgende week donderdag, als morgen niet meer lukt.

Prima. Maar ik ben al redelijk leeg gelopen.

Tot slot: misschien kunnen jullie je voorstellen dat als je alles op alles te zet om iedereen te bedienen, alles oplijnt om zo open mogelijk het debat te zoeken, juist die partijen kiest om zo goed mogelijk de kwaliteit te borgen, maximaal inspanning levert alles goed te regelen op hoog niveau, vakanties en privegebeurtenissen negeert om een hoger doel te dienen dat het dan wel erg naar is dat dingen nu zo lopen. Op geen moment is er een sfeer geweest van 'dit houden we maar even achter'. Waarom zouden we? Bevindingen zijn om op te lossen: we willen van Corona af. Ik vrees alleen dat dit soort framing nu wel leidt tot nieuwe koudwatervrees om in de toekomst open te zijn bij de overheid.

Hartelijke groet,

5.1.2e

met vriendelijke groet,

5.1.2e

----- Original Message -----

From: "5.1.2e" <5.1.2e>

To: "5.1.2e ." <5.1.2e @umcutrecht.nl>, "5.1.2e "
<5.1.2e 5.1.2e 5.1.2e <5.1.2e @cwi.nl>

Cc: "5.1.2e 5.1.2e " <5.1.2e @minvws.nl>, "5.1.2e)"
<5.1.2e @minvws.nl>

Sent: Wednesday, September 30, 2020 5:51:53 PM

Subject: Re: Short call

Allen,

Natuurlijk met liefde. Mijn telefoonnummer is 5.1.2e.

Hartelijke groet,

5.1.2e

Op 30-09-2020 om 17:50 schreef 5.1.2e .:

> Hoi 5.1.2e cc onze secretarissen,
>
> Ik heb vandaag contact gehad met 5.1.2e en een paar minuten geleden nog gesproken met de vraag of hij morgen tussen 14-16u in de cie 'langs' kon komen. Dat doet hij graag maar lukt hem morgen helaas niet. 5.1.2e gaf aan om nu direct met jullie 5.1.2e te bellen, zodat jullie vragen en opmerkingen direct besproken kunnen worden.
>
> Ik vind het netter jullie op deze wijze te linken, dan kunnen jullie zelf telefoonnummers uitwisselen. Pakken jullie drie dit verder op. Bedenk Zelf even of iemand anders nog zou moeten aanhaken.
>
> 5.1.2e - top dat je dit direct even wilt doen.

Met groet,

5.1.2e

De informatie opgenomen in dit bericht kan vertrouwelijk zijn en is

uitsluitend bestemd voor de geadresseerde. Indien u dit bericht onterecht

ontvangt, wordt u verzocht de inhoud niet te gebruiken en de afzender direct

te informeren door het bericht te retourneren. Het Universitair Medisch

Centrum Utrecht is een publiekrechtelijke rechtspersoon in de zin van de W.H.W.

(Wet Hoger Onderwijs en Wetenschappelijk Onderzoek) en staat geregistreerd bij

de Kamer van Koophandel voor Midden-Nederland onder nr. 30244197.

Denk s.v.p aan het milieu voor u deze e-mail afdrukt.

This message may contain confidential information and is intended exclusively

for the addressee. If you receive this message unintentionally, please do not

use the contents but notify the sender immediately by return e-mail. University

Medical Center Utrecht is a legal person by public law and is registered at

the Chamber of Commerce for Midden-Nederland under no. 30244197.