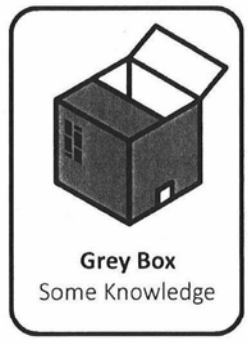
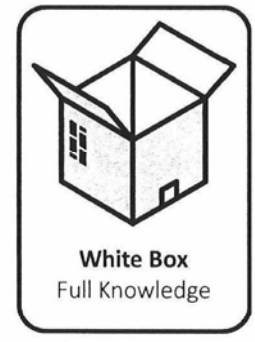
IT FORENSICS & INCIDENT RESPONSE

Offerte penetratietest



Grey Box
Some Knowledge



White Box
Full Knowledge

Organisatie:	Ministerie van Volksgezondheid, Welzijn en Sport T.a.v. (10)(2e) Parnassusplein 5 2511 VX Den Haag
Aangeboden via:	Nextcloud
Datum:	Den Haag, 22-06-2020
Betreft:	Penetratietest offerte COVID-19 Notification app + Infrastructuur

NL66ABNA 0253 0931 40

69575347 Den Haag

8579.24.953.B01

Verlengde Tolweg 2
2517 JV Den Haag
088 - 323 02 05
info@nfir.nl

IT FORENSICS & INCIDENT RESPONSE

Inhoudsopgave

Opdrachtomschrijving 3

Scope van de penetratietest 3

Timeboxed Grey Box onderdeel – App Infrastructuur, API en Meld / 4

Beheerportaal 4

Timeboxed White Box onderdeel – Mobiele applicaties (iOS & Android) 6

Tijdsverloop van de penetratietest 7

Rapportage 7

Gebruikte standaarden bij de uitvoering van deze penetratietest 8

CIA-bepalingen t.b.v CVSS-score 9

Algemene vereiste documenten en informatie voor de start 9

Opdracht specifieke vereisten voor de start 10

NFIR team 10

Tarieven en projectkosten 11

Bijlage 1: dienstenbeschrijving penetratietest 12

IT FORENSICS & INCIDENT RESPONSE

Geachte heer (10)(2e)

Op 15 juni 2020 spraken mijn collega (10)(2e) (10)(2e) en ik tijdens de aangename kennismaking en intake met de (10)(2e) en de (10)(2e) over de penetratietest die het Ministerie van VWSwil laten uitvoeren door NFIR. Het ministerie heeft aangegeven graag de technische weerbaarheid van de COVID-19 Notification app te laten testen.

In deze offerte treft u de opdrachtomschrijving, een uitwerking van de scope per te testen onderdeel, onze aanpak, de gebruikte standaarden en de vereisten voor de start van dit project. Tot slot treft u een urencalculatie van de onderdelen van deze pentest met onze tarieven.

Opdrachtomschrijving

Het doel van deze pentest is inzicht krijgen in de huidige digitale veiligheidsstatus van de COVID-19 Notification app en de bijbehorende extern beschikbare infrastructuur. Het Ministerie van VWS gaat de pentest rapportage gebruiken om gevonden kwetsbaarheden op te lossen op basis van de geprioriteerde CVSS scores die worden opgenomen in de rapportage.

Scope van de penetratietest

Door het Ministerie van VWSis documentatie aangeleverd over de tijdens de intake besproken scope van deze penetratietest. Dit omvatte informatie over de publiek beschikbare omgevingen, de netwerk infrastructuur, de API-structuur en de broncode van de mobiele applicaties. De volgende bestanden en bronnen zijn door ons ontvangen en bestudeerd:

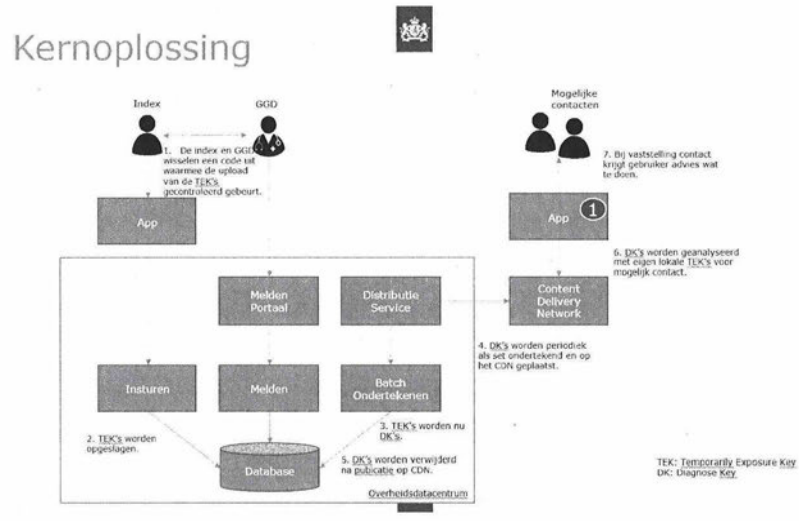
- Exposure Notificatie Infrastructuur Overview.pptx
- Covid-19 App Crypto Raamwerk 0.60.docx
- Solution architecture - https://github.com/minvws/nl-covid19-notification-app-coordination/blob/master/architecture/Solution%20Architecture.md
- OpenAPI Specification - https://github.com/minvws/nl-covid19-notification-app-coordination/tree/master/architecture/api
- iOS app (source code) - https://github.com/minvws/nl-covid19-notification-app-ios
- Android-app (source code) - https://github.com/minvws/nl-covid19-notification-app-android
- App back-end (source code) - https://github.com/minvws/nl-covid19-notification-app-backend

De informatie in deze documenten vormt de basis voor de inschatting van de pentest. De door uw organisatie verstrekte informatie en de verkregen informatie tijdens het intakegesprek zijn gebruikt voor de bepaling van de scope en de ureninschatting van deze opdracht.

IT FORENSICS & INCIDENT RESPONSE

Timeboxed Grey Box onderdeel – App Infrastructuur, API en Meld / Beheerportaal

Voor het timeboxed Grey Box onderdeel is de volgende informatie ontvangen over de publiek beschikbare infrastructuur en API's welke door de COVID-19 Notification app worden gebruikt. Daarbij is de volgende schematische weergave door opdrachtgever verstrekt over de oplossing:



Verstrekte API-requests

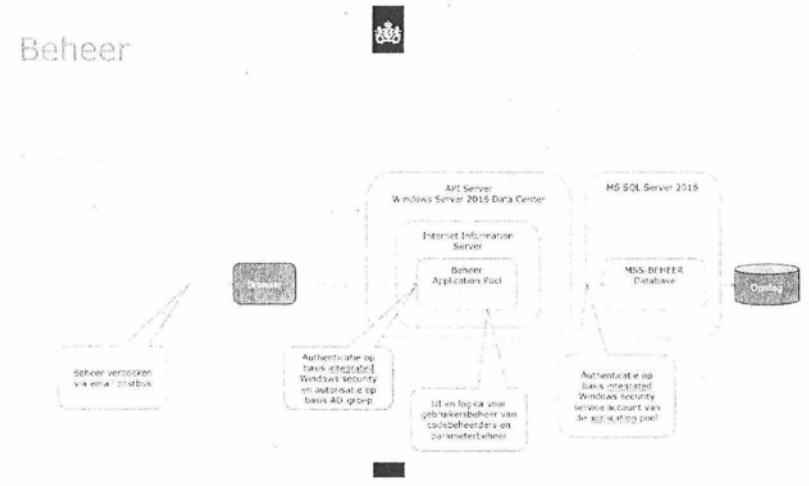
Door opdrachtgever zijn door middel van OpenAPI documentatie de volgende API-requests voor de mobiele applicaties verstrekt:

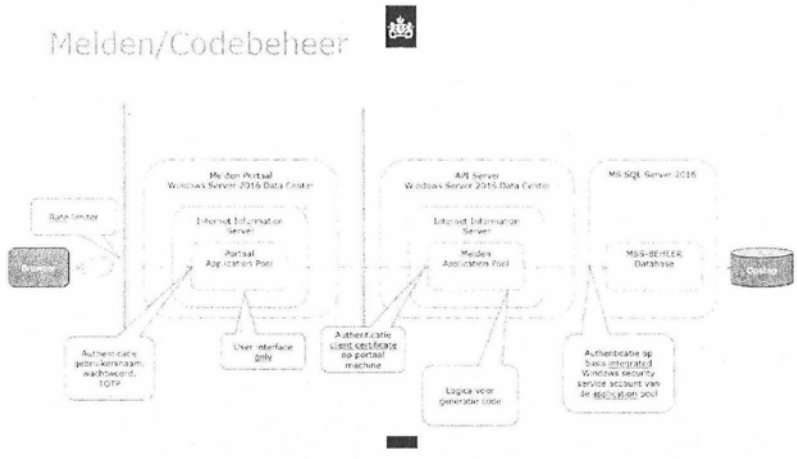
- /manifest.json
- /exposurekeyset/{id}
- /resourcebundle/{id}
- /riskcalculationparameters/{id}.json
- /appconfig/{id}.json
- /register
- /labconfirm
- /postkeys
- /stopkeys

IT FORENSICS & INCIDENT RESPONSE

Beheer/meldportaal

Door opdrachtgever is door middel van documentatie de volgende schematische weergave met betrekking tot het beheer- en meldportaal verstrekt:





Gedurende het Greybox aanvalsperspectief van de infrastructuur, zal deels gebruik worden gemaakt van de verstrekte authenticatiemethodes. Met behulp van verschillende technieken, zoals Open Source Intelligence (OSINT), wordt getracht informatie te verkrijgen over de infrastructuur, het beheerportaal en de API's om zo mogelijke kwetsbaarheden te ontdekken.

Timeboxed White Box onderdeel – Mobiele applicaties (iOS & Android)

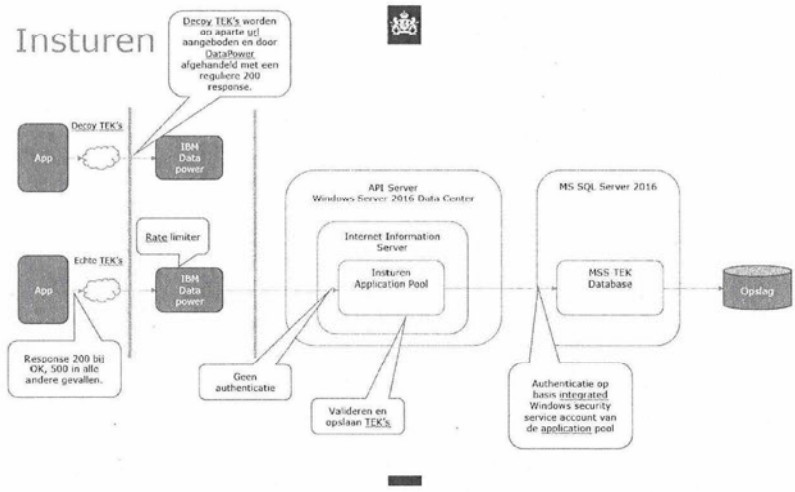
Voor het Timeboxed White Box onderdeel is informatie ontvangen over de omgevingen. Deze informatie vormt de basis voor de pentest op de interne en de publiek beschikbare omgeving.

De volgende applicaties zullen (op basis van de ontvangen informatie) onderzocht worden:

- COVID-19 Notification app – iOS https://github.com/minvws/nl-covid19-notification-app-ios
- COVID-19 Notification app - Android - https://github.com/minvws/nl-covid19-notification-app-android

De hierboven gespecifieerde mobiele applicaties vallen binnen de scope van de penetratietest, waarbij de focus zal liggen op het bepalen van de digitale veiligheidsstatus van de mobiele applicatie en de koppeling met de back-end.

Daarbij zal specifiek onderzoek gedaan worden naar de aanwezige functies binnen de mobiele applicatie. Ook zal worden gekeken naar de veiligheidsstatus van het insturen van zogenoemde TEKs van een besmet persoon:



Daarnaast zal worden gekeken naar aanvalsscenario's waarbij informatie kan worden beïnvloed binnen de applicatie (onterecht triggeren van notificaties via de mobiele applicaties, onterecht niet triggeren van notificaties via de mobiele applicaties). Ook zal onderzocht worden of er zich kwetsbaarheden voordoen in lijn met de OWASP Mobile Security Testing Guide (MSTG).

Uitgebreidere informatie over de uitvoering van de penetratietest treft u in Bijlage 1: dienstenbeschrijving pentest.

Tijdsverloop van de penetratietest

Allereerst zal gestart worden met het GreyBox aanvalsperspectief van de extern bereikbare applicaties. Dit onderdeel zal op afstand worden uitgevoerd. Vervolgens zal overgegaan worden op het Whitebox aanvalsperspectie op de mobiele applicaties waarbij de aangeleverde broncode gebruikt zal worden om kwetsbaarheden sneller vast te kunnen stellen.

Rapportage

De bevindingen tijdens deze opdracht worden gedocumenteerd in een heldere en volledige rapportage. Indien deze pentest bestaat uit verschillende onderdelen, zullen de bevindingen per onderdeel worden gerapporteerd. De rapportage wordt altijd gereviewd door een OSCP/eWPT gecertificeerd ethisch hacker. De rapportage zal worden uitgebracht in de Nederlandse taal. De rapportage zal worden opgeleverd via de beveiligde deelomgeving, waarbij een wachtwoord benodigd is om het document te downloaden. Dit wachtwoord sturen wij naar het 06-nummer van de ontvanger(s). Wij verzoeken u daarom in de tabel onder 'Algemene vereiste documenten en informatie voor de start' aan te geven aan wie de rapportage opgeleverd dient te worden en wat de contactgegevens van de ontvangers zijn.

De opleverdatum van de rapportage zal tijdig aan u worden doorgegeven. Na oplevering en bestudering van de rapportage zullen wij een toelichting geven op de bevindingen en heeft u alle gelegenheid om vragen te stellen. Wij nemen na oplevering van de rapportage contact met u op om deze afspraak in te plannen.

Gebruikte standaarden bij de uitvoering van deze penetratietest

Bij de pentest zal gebruik worden gemaakt van de diverse internationale standaarden voor het ontdekken en het classificeren van kwetsbaarheden. De standaarden die van toepassing zijn op deze opdracht:

- Penetration Testing Execution Standard (PTES): standaard ten behoeve van infrastructuur pentesten.
  - Meer informatie over deze standaard vindt u hier
  - De checklist voor deze standaard is toegevoegd als bijlage.
- Top 10: de 10 meest kritische kwetsbaarheden van webapplicaties.
  - Meer informatie over deze standaard vindt u hier

  OWASP WSTG: standaard ten behoeve van web applicatie pentesten.
  - Meer informatie over deze standaard vindt u hier
  - De checklist voor deze standaard is toegevoegd als bijlage.
- OWASP API Security Top 10: de 10 meest kritische kwetsbaarheden van API's.
  - Meer informatie over deze standaard vindt u hier
- OWASP MSTG: standaard ten behoeve van mobiele applicatie pentesten.
  - Meer informatie over deze standaard vindt u hier
  - De checklist voor deze standaard is toegevoegd als bijlage.
- Common Vulnerability Scoring System (CVSS): wordt gebruikt om de ernst van de kwetsbaarheden te classificeren.
  - Meer informatie over CVSS-calculator treft u hier

IT FORENSICS & INCIDENT RESPONSE

CIA-bepalingen t.b.v CVSS-score

Indien gewenst kan gebruik worden gemaakt van het CIA-model (Confidentiality, Integrity and Availability) om de technische risico-inschatting van de geteste omgevingen te beïnvloeden. De CVSS-score wordt door de CIA-bepaling bijgestuurd, zodat deze bij het bedrijfsrisico van uw organisatie aansluit. Mocht u gebruik willen maken van een CIA-bepaling dan verzoeken wij u de bijlage bij deze offerte ingevuld te retourneren voor de start van de pentest.

Algemene vereiste documenten en informatie voor de start

De volgende documenten en informatie zijn vereist voor het uitvoeren van deze opdracht:

- Een getekende versie van deze pentest offerte
- De getekende vrijwaringsverklaring voor deze opdracht. Deze wordt als bijlage bij deze offerte meegestuurd
- Een of meerdere contactpersonen van uw organisatie die beschikbaar is/zijn tijdens de pentest zodat de technical lead eventuele kritieke bevindingen direct kan doorgeven:

Naam	E-mailadres	Mobiel nummer

- Gegevens van de personen die na afloop van de pentest de rapportage dienen te ontvangen:

Naam	E-mailadres	Mobiel nummer

IT FORENSICS & INCIDENT RESPONSE

Opdracht specifieke vereisten voor de start

- Timeboxed GreyBox onderdeel – App Infrastructuur, API en Meld/beheerportaal:
  - Alle IP-addressen/hostnames welke onderdeel zijn van de infrastructuur
  - De endpoints en bijbehorende IP-addressen welke specifiek gebruikt worden voor het meld/beheerportaal
  - Twee (2) gebruikersaccounts voor het beheerportaal
  - Twee (2) gebruikersaccounts inclusief TOTP voor het meldportaal (Melden/Codebeheer)
  - Een CIA-bepaling per domein/IP-adres (zie bijlage indien gewenst)
  - Functionaliteitenlijst van het meld- en beheerportaal
- Ten behoeve van het Timeboxed WhiteBox onderdeel - Mobiele applicaties (iOS & Android):
  - Een CIA-bepaling per endpoint/mobiele applicatie/IP-adres (zie bijlage indien gewenst)
  - Gecompileerde varianten van de COVID-19 Exposure Notification mobiele applicaties voor
    - Apple iOS
    - Google Android
  - De endpoints en bijbehorende IP-adressen welke specifiek gebruikt worden door de mobiele applicaties
  - Additionele documentatie over hoe succesvolle HMAC shared-secret geimplementeerd worden en mogelijkheden om de implementatie te kunnen testen (bijv. genereren van een lijst met valide HMAC's voor de pentest) of vergelijkbaar.
- Voor de start van de Grey Box pentest dient u in de firewall onze IP-adressen (10)(2g) en (10)(2g) te whitelisten zodat de firewall NFIR niet blokkeert en de pentest onnodig stil komt te liggen.

NFIR team

De pentest zal worden uitgevoerd door eigen medewerkers van NFIR. Ons team bestaat uit zeer kundige ethische (white hat) hackers, digitaal forensisch onderzoekers, cyber security consultants, software ontwikkelaars en project leads. Wij zijn in het bezit van een POB vergunning van het ministerie van Veiligheid en Justitie (nummer 1672). Alle NFIR medewerkers hebben Korpschef goedkeuring en worden jaarlijks onderworpen aan een integriteitsonderzoek. Met deze status van betrouwbaarheid onderscheidt NFIR zich van vele andere cyber security specialisten.

IT FORENSICS & INCIDENT RESPONSE

Tarieven en projectkosten

Op basis van de hierboven beschreven scope en werkzaamheden is een urencalculatie gemaakt. In de onderstaande tabel treft u de werkzaamheden, het aantal uren (fixed) en onze tarieven.

Beschrijving van de pentest werkzaamheden	Uren	Uurtarief*	Subtotaal
Timeboxed Grey Box onderdeel – App Infrastructuur, API en Meld/beheerportaal	60	(10)(2b)	(10)(2b)
Timeboxed White Box onderdeel – Mobiele applicaties (iOS & Android)	80	(10)(2b)	(10)(2b)
Totaal incl. rapportage en een toelichting van de belangrijkste bevindingen van deze pentest. Exclusief een uit te voeren hertest.	140		(10)(2b)

* Indien de opdrachtgever deze pentest wil laten uitvoeren buiten kantoortijden dan is het uurtarief (10)(1c)

Op deze aanbieding zijn de algemene voorwaarden van NFIR BV van toepassing. Deze zijn als bijlage bij deze offerte toegevoegd. Bij de start van het project zal 50% van deze offerte gefactureerd worden. De overige 50% wordt gefactureerd bij oplevering van de rapportage. Alle genoemde tarieven zijn excl. 21% BTW. De betalingstermijn is 14 dagen netto.

Mochten er naar aanleiding van deze offerte nog vragen zijn of u heeft de behoefte aan een toelichting dan vernemen wij dat uiteraard graag. Indien u akkoord gaat met deze offerte dan verzoeken wij u de getekende versies van deze offerte en de vrijwaringsverklaring retour aan te bieden via de beveiligde Nextcloud omgeving die wij hebben aangeboden. Zodra wij uw officiële akkoord ontvangen zullen wij de werkzaamheden samen met u definitief inplannen.

Nogmaals dank voor uw aanvraag en wij kijken er naar uit om deze opdracht te mogen uitvoeren.

Met vriendelijke groet,

(10)(2e)

NFIR BV

(10)(2b) (10)(2e)

(10)(2e)

Voor akkoord,

(10)(2e)

(10)(2e)

(10)(2e) Ministerie van VWS

Naam: (10)(2e)

(10)(2e)

Datum: 26-06-2020

NFIR
IT FORENSICS & INCIDENT RESPONSE

Bijlage 1: dienstenbeschrijving penetratietest

Inleiding

Het doel van een penetratie test is kwetsbaarheden vinden binnen de afgesproken scope en de daar bijbehorende infrastructuur. Hierbij zijn drie aanvalsperspectieven mogelijk om technische beveiligingsrisico's of misbruik van een IT-infrastructuur, web/mobiele applicatie, website en API's in kaart te brengen. De aanvalsperspectieven van het beveiligingsonderzoek zijn een Black Box, Grey Box of White Box (ook wel Crystal Box genoemd).

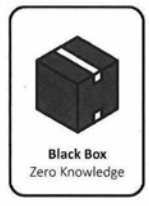
Aanvalsperspectieven

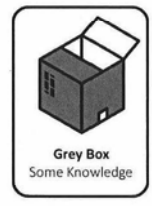
Een beveiligingsonderzoek op basis van het Black Box principe kan vergeleken worden met een echte aanval, zoals hackers (Black hat) deze zouden uitvoeren. Er is vooraf dan ook geen informatie verstrekt door de opdrachtgever. Onze ethische hackers zullen onder andere middels open bronnen onderzoek (OSINT) uw omgeving in kaart brengen om vervolgens op zoek te gaan naar technische kwetsbaarheden.

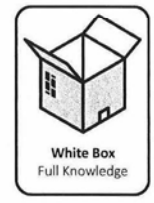
Bij een Grey Box aanvalsperspectief sporen ethisch hackers aan de hand van beperkte informatie kwetsbaarheden op in uw (web) applicatie, website, IT-infrastructuur, API-koppelingen en mobiele apps. Informatie die over de te testen scope ontvangen wordt, kan bijvoorbeeld bestaan uit gebruikersaccounts met standaardrechten waarbij de ethisch hackers zullen proberen meer rechten te krijgen of toegang te verkrijgen tot informatie die deze gebruiker niet in zou mogen zien.

Tot slot het White Box- principe (ook wel Crystal Box), waarbij vooraf alle informatie wordt verstrekt. Dit wordt gedaan met het idee om gericht op zoek te gaan naar kwetsbaarheden binnen de te testen scope. Denk hierbij aan source code, gedefinieerde scope, rollen/rechten matrix en functionaliteiten lijst.

Uiteraard is het mogelijk om een combinatie te maken van verschillende aanvalsperspectieven, om een zo compleet mogelijk beeld van de technische weerbaarheid van uw digitale omgeving te verkrijgen. Daarnaast kan de pentest als een Timeboxed variant worden uitgevoerd, waarbij binnen een vooraf afgesproken aantal uur zo veel mogelijk getest zal worden. Tijdens het intake gesprek wordt de scope vastgesteld, de gewenste (en passende) aanvalsperspectieven besproken en een vorm gekozen waarop de pentest wordt uitgevoerd.







IT FORENSICS & INCIDENT RESPONSE

Gebruikte standaarden bij de uitvoering van deze penetratietest

Om een succesvolle beveiligingsaudit uit te voeren, gebruikt NFIR verschillende internationale erkende standaarden voor het testen van informatiebeveiliging. De drie belangrijkste standaarden hierbij zijn:

- Penetration Execution Standard (PTES): standaard ten behoeve van infrastructuur pentesten.
- Open Web Application Security Project (OWASP):
  - Top 10 – de 10 meest kritische kwetsbaarheden van webapplicaties.
  - WSTG – Standaard ten behoeve van webaplicatie pentesten.
  - API Security Top 10 – De 10 meest kritische kwetsbaarheden van API's.
  - MSTG – Standaard ten behoeve van mobiele applicatie pentesten.
- Common Vulnerability Scoring System (CVSS): wordt gebruikt om de ernst de kwetsbaarheden te classificeren.

Door gebruik te maken van deze normen zorgt NFIR voor een complete en grondig uitgevoerd veiligheidsonderzoek.

Inzet van de NFIR Pentest Box

Voor Grey Box pentesten wordt onze Pentest Box ingezet. Dit is een volwaardige computer die in een handpalm past en geplaatst dient te worden achter de firewall in uw netwerk op kantoor of in het datacenter. De Pentest Box communiceert middels een VPN verbinding (versleuteld) via uw internet verbinding naar het pentest domein van NFIR, zodat de ethisch hackers op een beveiligde wijze toegang hebben tot uw netwerk zonder fysiek aanwezig te hoeven zijn. Indien de internetverbinding (tijdelijk) niet tot stand gebracht kan worden bieden wij een 4G-dongle die in de Pentest Box geplaatst kan worden en zorgt voor de noodzakelijke internetverbinding.

Whitelisten van NFIR IP adressen

(10)(1c)

(10)(1c) Het doel van de pentest is namelijk niet het controleren of compromitteren van de firewall, maar de server en/of applicaties achter de firewall.

CIA model

Een CIA-classificatie is een indeling die binnen de informatiebeveiliging wordt gehanteerd, waarbij de confidentiality (vertrouwelijkheid), integrity (integriteit) en availability (beschikbaarheid) van informatie en systemen wordt aangegeven. Opdrachtgevers kunnen middels het CIA-model aangeven of het verlies van vertrouwelijkheid, integriteit en beschikbaarheid van de informatie of systemen die binnen de te testen scope vallen, een high, medium of low impact heeft:

- High: Verlies heeft waarschijnlijk een catastrofaal nadelig effect op de organisatie of personen die aan de organisatie zijn gekoppeld (bijvoorbeeld werknemers, klanten).
- Medium: Verlies heeft waarschijnlijk een ernstig nadelig effect op de organisatie of personen die aan de organisatie zijn gekoppeld (bijvoorbeeld werknemers, klanten).
- Low: Verlies heeft waarschijnlijk slechts een beperkt nadelig effect op de organisatie of personen die aan de organisatie zijn gekoppeld (bijvoorbeeld werknemers, klanten).

IT FORENSICS & INCIDENT RESPONSE

Er zijn zeven fasen tijdens een penetratietest. Deze zeven fasen zijn:

Fase 1: Intelligence Gathering

Deze fase bestaat uit het verzamelen van zoveel mogelijk informatie uit beschikbare bronnen. Dit kunnen openbare bronnen (OSINT) zijn, zoals de WHOIS-database, de gebruikte DNS-servers, (sub)-domeinnamen, e-mail adressen en databases met gelekte wachtwoorden. Tevens kan informatie worden aangeleverd door de opdrachtgever, zoals netwerktekeningen en een IP nummerplan. Deze beschikbare bronnen hoeven niet noodzakelijkerwijs deel uit te maken van de van tevoren geïdentificeerde scope.

Fase 2: Threat Modelling

Gedurende deze fase wordt de informatie gewaardeerd en wordt daarmee vastgesteld welke informatie relevant is voor de penetratietest. U kunt hierbij denken aan het identificeren van waardevolle informatie, uitdenken van een aanvalsmethodiek en onderzoeken van de bedreigingen.

Fase 3: Vulnerability Analysis

Nadat alle informatie is verzameld, wordt in deze fase gezocht naar kwetsbaarheden in systemen en applicaties. Hierbij wordt gebruik gemaakt van tooling die automatisch zoekt naar bekende kwetsbaarheden. Daarnaast wordt door een ethische hacker op een creatieve wijze handmatig gezocht en gekeken naar kwetsbaarheden. Tijdens deze fase wordt gebruik gemaakt van diverse internationale standaarden zoals OWASP Top 10, PTES en OWASP MSTG.

Fase 4: Exploitation

Tijdens de exploitation fase is toegang verkrijgen tot het systeem het doel. De reeds verzamelde informatie wordt gebruikt om op een zorgvuldige wijze aanvallen uit te voeren. Deze aanvallen hebben als doel de geïdentificeerde kwetsbaarheden uit de vorige fase te bevestigen.

Fase 5: Post-Exploitation

In de post-exploitation fase wordt vastgesteld wat de waarde is van het gecompromitteerde systeem. Dit is afhankelijk van de gevonden data en of deze bruikbaar is om het netwerk verder te compromitteren.

Fase 6: Reporting

Alle bevindingen zullen worden samengebracht in een compleet en helder uitgewerkt rapport. Dit rapport bevat een beschrijving van de bevindingen, een scoresysteem (CVSS) waarbij de kwetsbaarheden een classificatie krijgen, de mogelijke impact van de kwetsbaarheden en aanbevelingen die uw organisatie helpen met het oplossen van de gevonden kwetsbaarheden.

Fase 7: Re-audit

Op basis van de aanbevelingen kunnen de gevonden kwetsbaarheden door uw eigen organisatie (of externe partij) worden opgelost. Zodra de kwetsbaarheden zijn opgelost, wordt NFIR veelal gevraagd dit te controleren middels een re-audit (hertest). Er wordt dan onderzocht en gerapporteerd of de kwetsbaarheden daadwerkelijk zijn opgelost. Op deze manier bent u verzekerd van een onpartijdig en scherp oordeel over de aangebrachte verbeteringen. U kunt de hertest rapportage bijvoorbeeld gebruiken om externe partijen (afnemers, partners, auditors, etc.) te overtuigen van de technische weerbaarheid van uw systemen en applicaties. Een hertest kan alleen worden begroot na voltooiing van de initiële penetratietest.

To: (10)(2e)](10)(2e) @minvws.nl]
Cc: (10)(2e)](10)(2e) @minvws.nl]; (10)(2e) .[(10)(2e) @minvws.nl]; (10)(2e) .
((10)(2e))[(10)(2e) @minvws.nl]
From: (10)(2e))
Sent: Fri 7/10/2020 2:09:58 PM
Subject: FW: deep dive IC opschaling
Received: Fri 7/10/2020 2:09:59 PM
20200710 presentatie deep dive opschalingsplan Covid-19.pptx

Ha (10)(2e)
De laatste vanuit cz! (10)(2e)

Verzonden met BlackBerry Work
(www.blackberry.com)

Van: (10)(2e) . < (10)(2e) @minvws.nl>
Datum: vrijdag 10 jul. 2020 3:49 PM
Aan: (10)(2e)) < (10)(2e) @minvws.nl>, (10)(2e)) < (10)(2e) @minvws.nl>, (10)(2e))
< (10)(2e) @minvws.nl>
Onderwerp: RE: deep dive IC opschaling

Hierbij aangepaste presentatie

Groeten (10)(2e)

(10 (10)(2e) (10)(2e)
Ministerie van Volksgezondheid, Welzijn en Sport | Directie Curatieve Zorg |
Parnassusplein 5 | 2511 VX | Den Haag | Postbus 20350 | 2500 EJ | Den Haag |
(10)(2e) (10)(2e)
(10)(2e) @minvws.nl | www.rijksoverheid.nl |

Van: (10)(2e)) < (10)(2e) @minvws.nl>
Verzonden: vrijdag 10 juli 2020 14:03
Aan: (10)(2e) . < (10)(2e) @minvws.nl>; (10)(2e)) < (10)(2e) @minvws.nl>; (10)(2e))
< (10)(2e) @minvws.nl>
Onderwerp: RE: deep dive IC opschaling

Ha (10)(2e) bedankt voor snelle actie.
Ik zou het korter willen maken

- derde sheet (Ic cap) weglaten
- opleiding personeel sheet korter (niet hele tabel)
- coördinatie en spreiding niet die hele illustratie opnemen. Wel graag specifiek noodzaak patiëntenspreiding regionaal en landelijk. En dat daar ook iets voor moeten regelen. Idem voor ict systeem beddeninzicht dat nodig is voor spreiding. En dat dat ook energie en geld kost.
- afspraken Duitsland zou ook korter kunnen denk ik.

(10)(2e)

Verzonden met BlackBerry Work
(www.blackberry.com)

Van: (10)(2e) . < (10)(2e) @minvws.nl>
Datum: vrijdag 10 jul. 2020 12:51 PM
Aan: (10)(2e)) < (10)(2e) @minvws.nl>, (10)(2e)) < (10)(2e) @minvws.nl>, (10)(2e))
< (10)(2e) @minvws.nl>
Onderwerp: deep dive IC opschaling

Hoi

Hierbij de presentatie voor de deep dive over de opschalingsplannen van het LNAZ op vrijdag 17 juli
Omdat dit het enige onderwerp heb ik het wat uitgebreider gedaan. Laat maar weten of het anders moet

Als deze deepdive (van 13.00-14.15) omgeruild kan worden met deepdive reguliere zorg in coronatijd (14.15-15.30) dan kan ik er bij zijn en de presentatie ook geven.
buiten verzoek
buiten verzoek

Groeten (10)(2e)

(10 (10)(2e) (10)(2e)
Ministerie van Volksgezondheid, Welzijn en Sport | Directie Curatieve Zorg |
Parnassusplein 5 | 2511 VX | Den Haag | Postbus 20350 | 2500 EJ | Den Haag |
(10)(2e) | (10)(2e)
(10)(2e) @minvws.nl | www.rijksoverheid.nl |

Reactie advies 2: Gebruik Google en Apple API

Reactie op advies 2 Begeleidingscommissie Digitale Ondersteuning Bestrijding Covid-19

9 juli 2020

"Gelet op het voorgaande adviseert de Begeleidingscommissie de Minister van VWS om met Google en Apple een verwerkersovereenkomst als bedoeld in artikel 28 van de Algemene verordening gegevensbescherming te sluiten. De begeleidingscommissie adviseert om in die verwerkersovereenkomst op te nemen dat Google en Apple garanderen dat zij geen gegevens, -op welke manier dan ook verzameld- in het kader van het gebruik van de notificatie-app zullen verwerken voor eigen doeleinden, óók niet wanneer functionaliteit van de notificatie-app in de besturingssystemen en/of software van Google en Apple zèlf ingebouwd zal worden."

Reactie: Om gebruik te kunnen maken van de notificatie app moeten gebruikers, afhankelijk van het type smartphone waarvan gebruik wordt gemaakt, deze downloaden uit de Apple App Store (iOS) of Google Play Store (Android). De beide downloadomgevingen zijn zoals bekend naar hun aard publiek beschikbaar.

Om de ontwikkeling van de app mogelijk te maken hebben Apple en Google een API ontwikkeld.[1] Deze API maakt mogelijk dat de app op basis van het DP3T protocol[2] kan functioneren op hun besturingssystemen (iOS resp. Android). De API en het systeem waarvan de API onderdeel uitmaakt zijn zo ontworpen en opgezet dat Apple en Google geen toegang kunnen hebben tot de gegevens die betrekking hebben op de gebruikers. Dit blijkt uit de documentatie die Apple en Google daarover hebben bekendgemaakt. Aldus het document Exposure Notification. Frequently Asked Questions, v1.1, May 2020:[3]

- The system was also designed so that Apple and Google do not have access to information related to any specific individual.

- In keeping with our privacy guidelines, Apple and Google will not receive identifying information about the user, location data, or information about any other devices the user has been in proximity of.

De implementatiesoftware van het DP3T protocol verwerkt de TEKs, DKs en RPIs/contactcodes, én kan een risicoscore bepalen aan de hand van een in de app opgenomen set parameters en weegfactoren. De parameters en weegfactoren worden vastgesteld door VWS, in overleg met RIVM, GGD-en en OMT, en kunnen op basis van nieuwe (wetenschappelijke) inzichten periodiek worden aangepast.

Er is sprake van de verwerking van (pseudonieme) persoonsgegevens (RPIs/contactcodes) van betrokkene op de smartphones van andere gebruikers, en de verwerking van gedownloade DKs en op basis daarvan gegenereerde (berekende) contactcodes. Deze gegevens zijn niet toegankelijk voor Apple en Google.

Apple en Google zijn daarmee partijen die betrokken zijn, maar niet zelfpersoonsgegevens verwerken. Het sluiten van een verwerkersovereenkomst met Apple en Google is daarom niet van toepassing, zij zijn immers geen verwerker.

---

[1] De documentatie over de door Apple en Google ontwikkelde API's is te vinden via www.apple.com/covid19/contacttracing (laatst. geraadpl. 1 juli 2020): Exposure Notification. FAQ, v1.1 May 2020; Exposure Notification. Cryptography Specification, v1.2 April 2020; Exposure Notification. Bluetooth Specification, v1.2, April 2020.

[2] DP3T wordt omschreven als "a secure, decentralized, privacy-preserving proximity tracing system. Its goal is to simplify and accelerate the process of identifying people who have been in contact with an infected person, thus providing a technological foundation to help slow the spread of the SARS-CoV-2 virus. The system aims to minimise privacy and security risks for individuals and communities and guarantee the highest level of data protection." De documentatie over DP3T is te vinden in het DP3T Repository op https://github.com/DP-3T/documents (laatst. geraadpl. 1 juli 2020).

[3] Exposure Notification. Frequently Asked Questions, v1.1, May 2020, par. 6 en 7, te vinden via www.apple.com/covid19/contacttracing (laatst. geraadpl. 1 juli 2020

"Voor Android toestellen wordt om de notificatie-app te laten functioneren als voorwaarde gesteld dat geolocatie wordt aangezet. De Begeleidingscommissie adviseert de Minister van VWS bovendien om in de verwerkersovereenkomst met Google op te nemen dat gebruikers van Android toestellen niet verplicht worden om geolocatie aan te zetten, nu geolocatie niet noodzakelijk is voor het functioneren van de app."

Reactie: Dit ligt iets genuanceerder:
Google heeft de interpretatie dat het gebruik van Bluetooth kan leiden tot identificatie van objecten waarvan de locatie bekend is. Wie zo'n database raadpleegt kan dan weten waar men ongeveer is. Om die reden vraagt google hiervoor toestemming. De toestemming houdt niet in dat google vervolgens GPS gebruikt om de locatie bij te houden.

Apple volgt de stelling van google niet. Apple geeft aan dat de beschreven situatie waarvoor google toestemming vraagt niet mag en straft daarop. Google doet dit niet. Vandaar dat google toestemming zo heeft ingeregeld. E.e.a. is in bijgevoegde paper uiteengezet en wordt bovendien op Europees niveau besproken.

Zoals op het eerste punt uiteengezet is, zijn Apple en Google geen verwerker en hebben Apple en google reeds in het document exposure notification vermeldt dat zij geen toegang tot dergelijke gegevens. Het nader regelen is daarmee niet nodig.

"Bovenstaande geldt zowel voor de notificatie-app die wordt ontwikkeld in de context van COVID-19 alsook voor een eventuele toekomstige situatie waarin een notificatie-app in de besturingssystemen en/of software van Google en Apple zèlf ingebouwd zal worden."

Reactie: Beide bedrijven hebben in hun mondelinge technische briefings een mogelijke fase twee ter sprake gebracht waarin vrijwel de gehele app functionaliteit `verdwijnt' in het besturingssysteem en geassocieerde software. Het is bij deze mondeling verstrekte technische informatie gebleven. Vragen rond data verzameling, verwerking en toegang konden niet door de technische vertegenwoordigers beantwoord worden. Op dit moment heeft geen van de twee partijen deze plannen in een voldoende uitgewerkte en gedocumenteerde versie gedeeld om hier een analyse van te kunnen maken. Vragen hierover spelen bij meerdere landen. Gesprekken hierover worden dan ook op Europees niveau ingezet.

"De Begeleidingscommissie adviseert de Minister van VWS om – gegeven het maatschappelijk belang van de volksgezondheid, waartoe gebruik van de COVID-app kan bijdragen, de gevoelige aard van de gegevensverwerking en de schaal waarop gegevens zullen worden verwerkt – de Autoriteit Persoonsgegevens te verzoeken om toezicht te houden op zorgvuldige naleving van de regels ter bescherming van persoonsgegevens door alle bij de COVID-app betrokken partijen, inclusief Google en Apple."

Reactie: Het is de taak van de Autoriteit Persoonsgegevens om toezicht te houden op zorgvuldige naleving ter bescherming van persoonsgegevens van alle verwerkingen. Zo ook op de verwerkingen in het kader van de Covid-19 app. Het is echter niet aan de minister van VWS om te sturen op prioriteiten van de AP als onafhankelijke toezichthouder. Gedurende het gehele traject is regelmatig contact met de AP over de voortgang van de app. Er is afgesproken dat de minister van VWS de DPIA aan hen voorlegt ter advies en toegezegd dat de minister het advies van de AP betrekt in zijn afwegingen.

"Ten slotte adviseert de Begeleidingscommissie om dit onderwerp in Europees verband aan te kaarten omdat dit probleem ook in andere EU-lidstaten voor Nederlandse ingezetenen en ingezetenen van andere lidstaten kan ontstaan. Tegelijkertijd adviseert de Begeleidingscommissie om vooral niet te wachten op een gemeenschappelijk Europees standpunt en onverwijld zelf contact op te nemen met Google en Apple. Met name gezien het beoogde tijdpad van de pilot met de COVID-19 notificatie-app."

Reactie: Zowel in Europees verband als op nationaal niveau is doorlopend overleg met Apple en Google. Dit zal actief worden voortgezet.

To: (10)(2e))[(10)(2e) @minvws.nl]
From: (10)(2e))
Sent: Wed 7/22/2020 2:00:12 PM
Subject: RE: virtueel bezoek maandag 27 juli
Received: Wed 7/22/2020 2:00:13 PM

Zo maar doen dan. thx

Groet,
(10)(2e) (10)(2e)
Department of International Affairs
Ministry of Health, Welfare and Sport
(10)(2e) (10)(2e) @minvws.nl

Van: (10)(2e)) < (10)(2e) @minvws.nl>
Verzonden: woensdag 22 juli 2020 15:59
Aan: (10)(2e)) < (10)(2e) @minvws.nl>
CC: (10)(2e)) < (10)(2e) @minvws.nl>; (10)(2e)) < (10)(2e) @minvws.nl>
Onderwerp: RE: virtueel bezoek maandag 27 juli

Hallo (10)(2e)
Wat betreft de context: IC-zorg is onderdeel van de reguliere ziekenhuiszorg en dit wordt normaliter bekostigd uit de zorgverzekeringswet en gecontracteerd door zorgverzekeraars. Vanuit de overheid hebben we normaliter niets van doen met de IC-bedden (net zoals we niet gaan over alle andere onderdelen in het zorgaanbod van de Zvw, dat is allemaal privaat georganiseerd). Omdat er vanwege de corona-pandemie buitengewone vraag is (geweest) naar IC-capaciteit, en dat in het normale systeem niet zomaar opgeschalad kon worden, zijn we hier vanuit de overheid bij betrokken geraakt.

Groeten, (10)(2e)

Van: (10)(2e)) < (10)(2e) @minvws.nl>
Verzonden: woensdag 22 juli 2020 15:55
Aan: (10)(2e)) < (10)(2e) @minvws.nl>
CC: (10)(2e)) < (10)(2e) @minvws.nl>; (10)(2e)) < (10)(2e) @minvws.nl>
Onderwerp: RE: virtueel bezoek maandag 27 juli

Hoi (10)(2e)

Dank voor je reactie. Hier wordt deze vraag ook maar gedropt dus we moeten het maar even snel zien op te leveren.

Ik ga kijken of ik hiermee via knippen en plakken uit de voeten kan.

Wat ik nog wel mis is een paar zinnen over de context van ons zorgsysteem en de plek van de IC-capaciteit daarin kort te schetsen. Nuttig voor onze net nieuwe (10)(2e)
Kan je dat nog verzorgen of wellicht ook hier een bestaand document sturen waaruit ik kan putten?

Groet,
(10)(2e) (10)(2e)
Department of International Affairs
Ministry of Health, Welfare and Sport
(10)(2e) (10)(2e) @minvws.nl

Van: (10)(2e)) < (10)(2e) @minvws.nl>
Verzonden: woensdag 22 juli 2020 15:28
Aan: (10)(2e)) < (10)(2e) @minvws.nl>
CC: (10)(2e)) < (10)(2e) @minvws.nl>; (10)(2e)) < (10)(2e) @minvws.nl>
Onderwerp: RE: virtueel bezoek maandag 27 juli

Hallo (10)(2e)
Het is nogal kort dag, midden in het reces en aan onze kant erg druk met de IC-opschalingsplannen, dus vind jet het goed dat ik je nu kortheidshalve het IC-opschalingsplan van het Landelijk netwerk Acute Zorg stuur, met daarbij de reactie van M MZS daarop aan de Kamer? Daarin staat exact het antwoord op je vragen (wat waren de lessen en wat is de focus voor de komende maanden).

Groeten, (10)(2e)

Van: (10)(2e)) < (10)(2e) @minvws.nl>
Verzonden: woensdag 22 juli 2020 14:37
Aan: (10)(2e)) < (10)(2e) @minvws.nl>
CC: (10)(2e)) < (10)(2e) @minvws.nl>; (10)(2e)) < (10)(2e) @minvws.nl>
Onderwerp: FW: virtueel bezoek maandag 27 juli

Beste (10)(2e)

Ik heb (10)(2e) proberen te bereiken maar ik zie dat hij op vakantie is. Daarom kom ik nu bij jou uit. Ik probeerde je net ook even te bellen maar je was in gesprek. Ik probeer het straks nog wel een keer maar toch alvast een verzoek via de mail.

Volgende week maandag heeft de (10)(2e) een gesprek met de (10)(2e) van de UK. Hij heeft aangegeven over een aantal concrete punten met de (10)(2e) te willen praten. Zie bijgevoegde mailwisseling
Één daarvan is de IC-capaciteit. Mag ik jou vragen of je daarvoor een bijdrage bij mij kunt aanleveren, uiterlijk donderdag 12u? Omdat de (10)(2e) pas nieuw is, is het ook nuttig om naast een reactie op de spreekpunten ook de context van ons zorgsysteem en de plek van de IC-capaciteit daarin kort te schetsen.

Alvast bedankt.

Groet,
(10)(2e); (10)(2e)
Department of International Affairs
Ministry of Health, Welfare and Sport
(10)(2e) (10)(2e) @minvws.nl

Van: (10)(2e) (Sensitive) < (10)(2e) @fco.gov.uk>
Verzonden: woensdag 22 juli 2020 13:12
Aan: (10)(2e)) < (10)(2e) @minvws.nl>
Onderwerp: RE: virtueel bezoek maandag 27 juli

Hoi (10)(2e)

Hartelijk dank voor de CV van (10)(2e) Bij deze de specifiekere punten waar de focus van het gesprek op zal liggen:

- De belangrijkste leermomenten met betrekking tot de intelligente lockdown. En de wetenschappelijke focus die hierbij genomen is op specifieke risicovlakken om de R rate onder controle te krijgen. De Nederlandse en Britse aanpak van de afgelopen maanden.
- Intensive care capaciteiten, wat is er geleerd van de druk waaronder de IC's hebben gestaan voor de komende winter maanden.
- Waar zal de focus liggen voor VWS naast IC capaciteit en personeel in de herfst.

Is het al bekend of MS Teams gebruikt kan worden? Anders zal ik het los navragen.
Groet,
(10)(2e)

(10)(2e) (10)(2e) **The Hague**
British Embassy | Lange Voorhout 10 | 2514 ED | The Hague | The Netherlands
+ (10)(2e) (10)(2e) @fco.gov.uk

UK in the Netherlands: GOV.UK | Facebook | Twitter | LinkedIn

travel aware Stay informed and check gov.uk/foreign-travel-advice