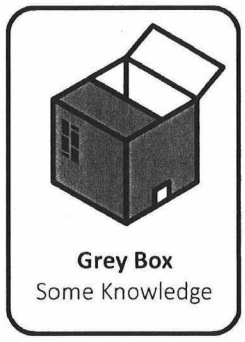
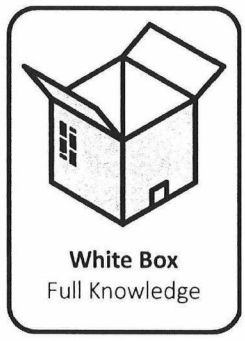
IT FORENSICS & INCIDENT RESPONSE

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

NL56ABNA 0253 0931 40
69575347 Den Haag
8579.24.953.B01

Verlengde Tolweg 1
2617 JV Den Haag
083 - 323 02 05
info@nfir.nl

IT FORENSICS & INCIDENT RESPONSE

Inhoudsopgave

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:

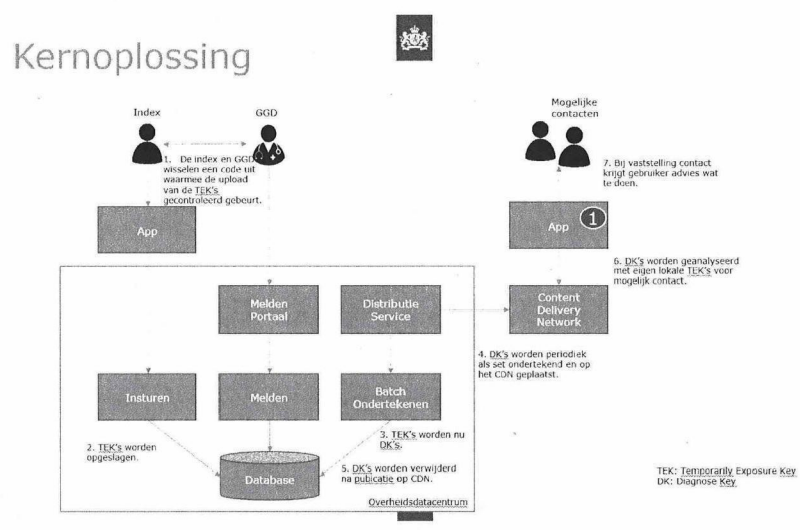
- Exposure Notificatie Infrastructuur Overview.pptx
- Covid-19 App Crypto Raamwerk 0.60.docx
- Solution architecture - https://github.com/minvws/nl-covid19-notification-app-coordination-dashboard/blob/master/architecture/Solution%20Architecture.md
- OpenAPI Specification - https://github.com/minvws/nl-covid19-notification-app-coordination-dashboard/tree/master/a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



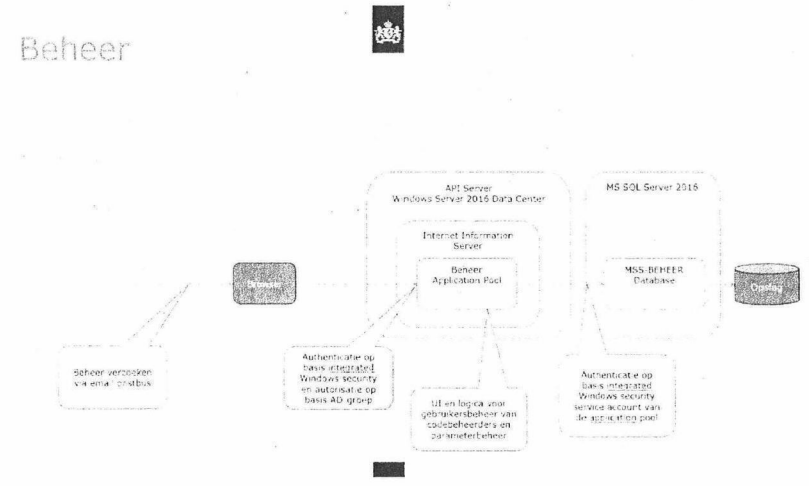
Verstrekte API-requests

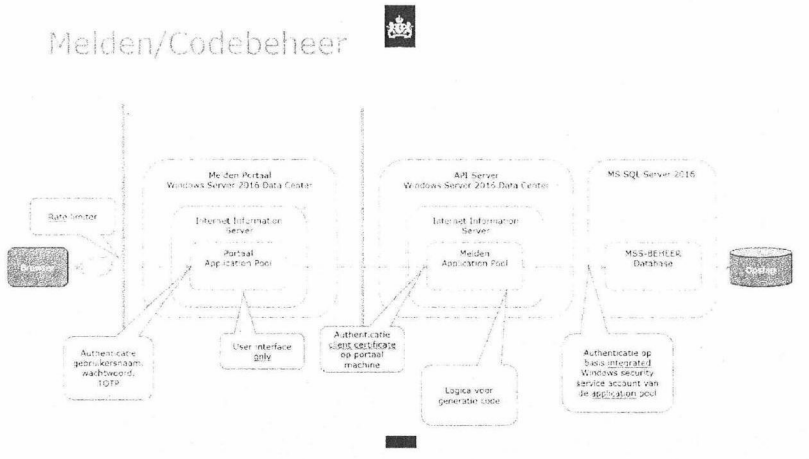
Door opdrachtgever zijn door middel van OpenAPI documentatie de volgende API-requests voor de mobiele applicaties verstrekt:

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

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)

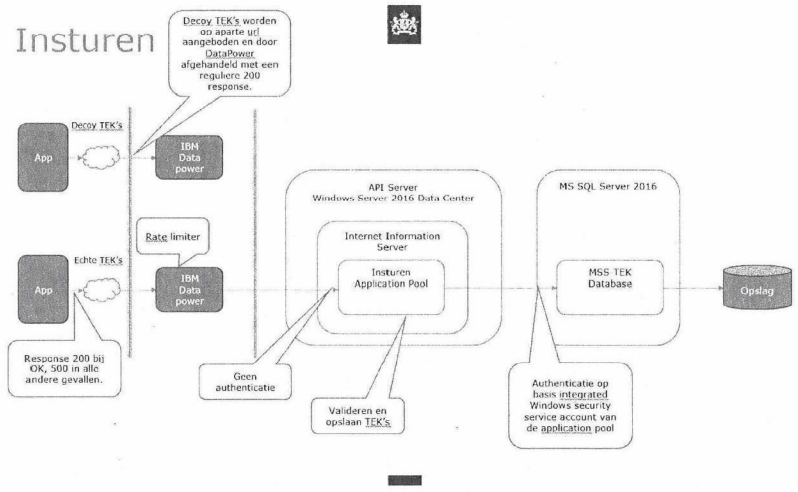
Voor het Timeboxed White Box onderdeel is informatie ontvangen over de omgevingen. Deze informatie vormt de basis voor de pentest op de interne en de publiek beschikbare omgeving.

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

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).

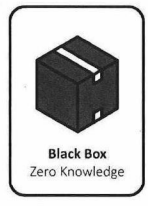
Aanvalsperspectieven

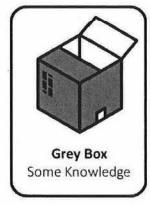
Een beveiligingsonderzoek op basis van het Black Box principe kan vergeleken worden met een echte aanval, zoals hackers (Black hat) deze zouden uitvoeren. Er is vooraf dan ook geen informatie verstrekt door de opdrachtgever. Onze ethische hackers zullen onder andere middels open bronnen onderzoek (OSINT)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

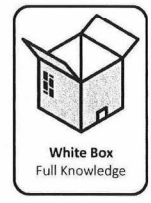
Bij een Grey Box aanvalsperspectief sporen ethisch hackers aan de hand van beperkte informatie kwetsbaarheden op in uw (web) applicatie, website, IT-infrastructuur, API-koppelingen en mobiele apps. Informatie die over de te testen scope ontvangen wordt, kan bijvoorbeeld bestaan uit gebruikersaccounts 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.