



# PENTEST MANAGEMENT SAMENVATTING

**Blackbox + Greybox Infrastructuur**

Opdrachtgever:	Humankind
Project:	24203 - Montese
Auteur(s):	M. van der Pol, M. Kamminga en N. Tocila
Reviewer(s):	S. van den Bent en P. Luijben
Document aangemaakt:	20-12-2024



Dit document mag niet worden verspreid of gekopieerd zonder toestemming van NFIR B.V.

NFIR B.V.  
Laan van Zuid Hoorn 165  
2289 DD Rijswijk

088-323 02 05  
info@nfir.nl  
www.nfir.nl

IBAN NL 81 RABO 0313 7904 93  
KVK 69575347  
BTW 8579.24.953.B01



## Disclaimer

### Vertrouwelijk

Dit document is geclassificeerd als vertrouwelijk. De informatie in dit document en de bijbehorende bijlagen zijn alleen bedoeld voor Humankind. Het gebruik van dit document door een andere partij dan hiervoor genoemd is niet toegestaan, tenzij deze partij uitdrukkelijk is geautoriseerd door Humankind. De informatie in dit document is als vertrouwelijk gemarkeerd en valt onder de bepalingen van een geheimhoudingsovereenkomst.

Als u het gepresenteerde document onbedoeld ontvangt en/of u hebt geen toestemming om het document in uw bezit te hebben, verzoekt NFIR B.V. u om het document onmiddellijk te sluiten en terug te sturen naar NFIR B.V.

Elk misbruik van dit document of de informatie in dit document is niet toegestaan. NFIR B.V. aanvaardt geen aansprakelijkheid voor enig ongeoorloofd gebruik of misbruik van het gepresenteerde document door een derde partij of voor schade veroorzaakt door de inhoud van dit document.

### Disclaimer Penetratietest

NFIR B.V. voert de penetratietest uit volgens de huidige normen en methodologieën. Een beveiligingscontrole is echter een momentopname. NFIR B.V. aanvaardt geen aansprakelijkheid voor kwetsbaarheden die niet (algemeen) bekend waren op het moment van het uitvoeren van de beveiligingsaudit.

### Copyright © 2024 NFIR B.V.

Alle rechten voorbehouden. De inhoud van dit document mag niet worden gedistribueerd, opgeslagen of gepubliceerd in welke vorm dan ook, digitaal, mechanisch, door fotokopie of opnames, zonder schriftelijke toestemming van NFIR B.V. Aanpassingen aan het door NFIR opgesteld rapport zijn op geen enkele wijze toegestaan.

### Handelsnamen

NFIR en het NFIR-logo zijn handelsmerken van NFIR B.V. Alle andere handelsmerken in dit document zijn eigendom van de vermelde partijen.

### Over NFIR

NFIR is een specialist in cyberbeveiliging. Bij NFIR zijn cyber-engineers in dienst: hackers die weten wat ze doen, testers die de werking van ICT-infrastructuren en software begrijpen, privédetectives die, indien nodig, onderzoeken kunnen uitvoeren, en adviseurs/consultants die u het juiste advies kunnen geven of die u kunnen ondersteunen bij een incident.

### POB-vergunning

Het ministerie van Justitie en Veiligheid heeft NFIR een vergunning afgegeven, waardoor NFIR haar werkzaamheden mag uitvoeren. Deze vergunning betreft de POB-vergunning. De POB-vergunning dekt het verwerken van strafrechtelijke gegevens, waarmee NFIR in aanraking kan komen bij het uitvoeren van haar diensten. Het POB-licentienummer van NFIR is: 1672.



## Management Samenvatting

Humankind heeft NFIR verzocht om een penetratietest uit te voeren op de interne/externe infrastructuur. De scope van de penetratietest omvatten de volgende items:

- Black Box -- Externe Infrastructuur (Timeboxed)
- Grey Box -- Interne Infrastructuur (Timeboxed)
- Grey Box -- Locatiebezoek (Timeboxed)

De penetratietest vond plaats van 09-12-2024 tot en met 27-12-2024. Deze gehele periode omvat zowel de technische uitvoering van de penetratietest als het samenstellen van dit rapport.

## Gebruikte standaarden bij de uitvoering van deze penetratietest

Bij de penetratietest is gebruikgemaakt van diverse internationale standaarden voor het ontdekken en classificeren van kwetsbaarheden. De volgende standaarden zijn van toepassing op deze opdracht:

- Penetration Testing Execution Standard (PTES): standaard ten behoeve van infrastructuur penetratietesten.
- Common Vulnerability Scoring System (CVSS): wordt gebruikt om de ernst van de kwetsbaarheden te classificeren.
- CWE (Common Weakness Enumeration): Lijst van veelvoorkomende softwarefouten voor het verbeteren van softwarebeveiliging.

## Aantal Bevindingen

Categorie	Bevindingen
<b>Bevindingen: Black Box – Externe Infrastructuur (Timeboxed)</b>	<ul style="list-style-type: none"><li>● Laag: 3 bevindingen</li><li>● Info: 5 bevindingen</li></ul>
<b>Bevindingen: Grey Box – Interne Infrastructuur (Timeboxed)</b>	<ul style="list-style-type: none"><li>● Hoog: 4 bevindingen</li><li>● Gemiddeld: 7 bevindingen</li><li>● Laag: 1 bevinding</li><li>● Info: 6 bevindingen</li></ul>
<b>Bevindingen: Grey Box – Locatiebezoek (Timeboxed)</b>	<ul style="list-style-type: none"><li>● Gemiddeld: 2 bevindingen</li></ul>

Tabel 1: Een overzicht van bevindingen gesorteerd op onderdeel.

Tijdens het onderzoek zijn in totaal 28 bevindingen aangetroffen waarvan 0 kritiek, 4 hoog, 9 gemiddeld, 4 laag en 11 informatief.



## Belangrijkste bevindingen

Hieronder worden de belangrijkste kwetsbaarheden kort benoemd.

1. **Hoog:** Via password spraying, een methode om één wachtwoord te proberen op alle gebruikers, is het wachtwoord van 94 gebruikers achterhaald.
2. **Hoog:** Daarnaast is via password spraying vastgesteld dat de gebruikersnaam (default) gelijk is aan het wachtwoord.
3. **Hoog:** Een registersleutel binnen de Group Policy van Humankind bevat AutoAdminLogon credentials van het account BSO.
4. **Hoog:** Het gebruik van multifactor-authenticatie (MFA) is niet verplicht voor alle gebruikers. Voor admin accounts is er een uitzondering gemaakt.

Tijdens het onderzoek is vastgesteld dat het niet mogelijk was om extern en intern toegang te verkrijgen tot de infrastructuur. Wel zijn er onveilige wachtwoorden aangetroffen.

## Adviezen

NFIR adviseert om de gevonden kwetsbaarheden zo spoedig mogelijk op te lossen in volgorde van hoog naar laag en een hertest uit te voeren om te verifiëren of de gevonden kwetsbaarheden daadwerkelijk zijn opgelost.

Daarnaast adviseert NFIR de opdrachtgever om zich te richten op de IT-security maatregelen, zoals omschreven in het hoofdstuk Adviezen .

