# Bijlage 2.1 Sjabloon onderzoeksverslag

Datum 4-6-2025

Auteur Farhan Muhammad

## Opdrachtgever

Securityofficer AmeRijck vakantiepark

## Managementsamenvatting

[Geef hier in het kort een samenvatting voor de directie met de aanleiding, de ondernomen acties, het resultaat, een conclusie en een advies.]

Er zijn 6 zwakheden gevonden. 1. Remote accesstool is geïnstalleerd en actief waardoor er op ongecontroleerde wijze toegang verkregen kan worden tot de databaseserver. 2. Het rootpassword van MYSQL is ‘root’. 3. Er is geen authentication afgedwongen in de database. 4. Firewall is uitgezet. 5. Antivirusbescherming is uitgezet. 6. Er is een virusinfectie. In uw server. Ondernomen acties zijn het encryptie gebruiken van remote accesstool, het root wachtwoord aangepast, een authentication in de database toegevoegd, Firewall aangezet voor extra beveiliging en antivirusbescherming aangezet om virussen te voorkomen. Wat ik had gemerkt is dat er een virus bestand is opgeslagen in uw server genaamd ‘admin.txt’ die heb ik zo snel mogelijk moeten verwijderen. Mijn advies is om al deze stappen te gaan volgen om ervoor te zorgen dat er geen zwakheden meer te zien krijgt.

## Overzicht onderzoek

[Een toelichting op wat onderzocht is en op welke manier.]

Er zijn 6 zwakheden die onderzocht moesten worden. 1. Remote accesstool is geïnstalleerd en actief waardoor er op ongecontroleerde wijze toegang verkregen kan worden tot de databaseserver. 2. Het rootpassword van MYSQL is ‘root’. 3. Er is geen authentication afgedwongen in de database. 4. Firewall is uitgezet. 5. Antivirusbescherming is uitgezet. 6. Er is een virusinfectie. Door gebruik te maken van bepaalde softwares en instellingen van windows.

### Wat is er onderzocht?

[Een beschrijving van de punten waarop controles zijn uitgevoerd.]

Wat ik heb onderzocht zijn de 6 zwakheden, wat ik heb gemerkt is dat tool geïnstalleerd en actief is.

Dat het rootpassword van MYSQL root is.

Geen strong authentication in de database.

Firewall uit staat.

Antivirusbescherming ook uit staat.

En dat er een virusinfectie is.(Virus gevonden admin.txt)

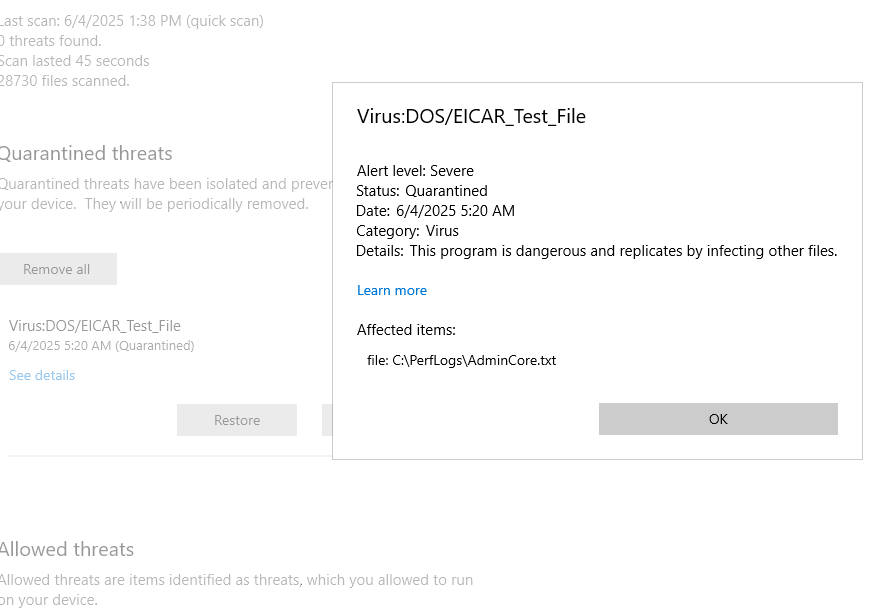
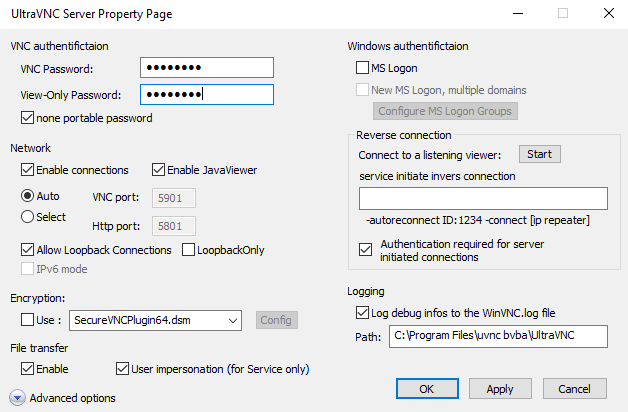
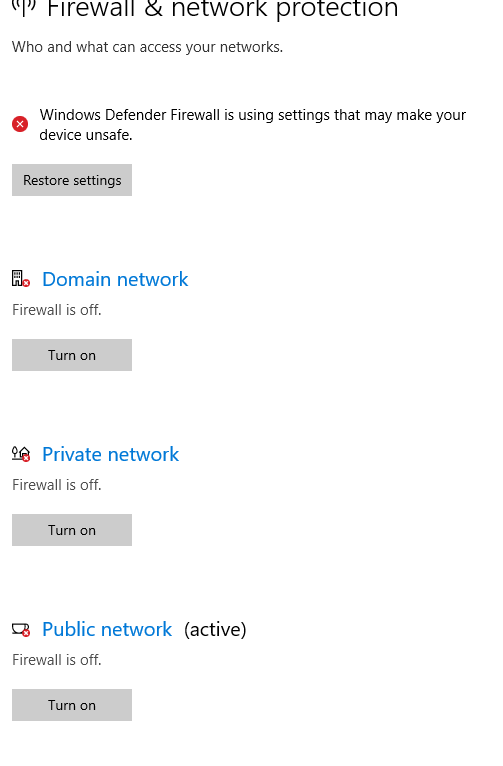
### Gevonden zwakheden

[Beschrijf de zwakheden met hun risiconiveau die mogelijk hebben bijgedragen tot het incident. Gebruik eventueel de matrix om dit overzichtelijk te rapporteren.]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Kans 🡺 | Risicomatrix | | | |
|  |  | x |  |
|  |  |  |  |
|  |  |  |  |
| Impact 🡺 | | | |

### Beschrijving gevonden bewijzen van eventueel misbruik

[Beschrijf welk *soort* bewijzen zijn gevonden.]

1. Ik heb hier een virus bestand gevonden
2. Geïnstalleerde tool 
3. Firewall die uitstaat

### Inhoud van gevonden bewijzen

[Beschrijf de relevante details van de bewijzen.]

Zoals uw aan de afbeeldingen kon zien zijn er bepaalde zwakheden gevonden. Virus bestand die om 5:20 in de ochtend gemaakt werd(toegevoegd), een remote accesstool die is geïnstalleerd en die maar niet weg wilt. En Firewall die uit stonden.

### Bericht mogelijk datalek

[Geef aan of en waarom er eventueel een melding gedaan moet worden bij het meldloket datalekken. Benoem hierbij welke gegevens mogelijk zijn gelekt en hoeveel personen hiervan mogelijk slachtoffer zijn.]

Er is geen eventuele datalekken die ik heb kunnen vinden. Enige wat wel een probleem is een tekst bestand genaamd ‘admin.txt’ die ik niet kan vinden in de map admin maar het bestaat wel en het is een virus bestand.

## Conclusie

[Beschrijf jouw conclusies. Neem ook een matrix met kans en impact op van de gevonden zwakheden.]

Kortom er zijn 6 zwakheden die ik heb gecontroleerd en beschreven wat er allemaal precies aan de hand is met bewijzen. Waar ik ook door middel van de zwakheden actie heb moeten ondernemen.

## Advies

[Geef adviezen op basis van jouw conclusies om tot een betere balans van werkbaarheid en veiligheid te komen voor de organisatie.]

Mijn advies is dat de geïnstalleerde remote accesstool te encrypten, ervoor zorgen dat root wachtwoord word aangepast naar een moeilijkere wachtwoord en beperk het aantal gebruikers die in root mogen komen, Zet de firewall aan voor voorkomende virussen zelfde geldt voor antivirusbescherming. In MYSQL de authentication policy aan te zetten om ervoor te zorgen dat het niet makkelijk wordt voor gebruikers zomaar als root in te loggen. En omdat er een virus bestand zit in uw server zorg ervoor dan dat antivirusbescherming aan staat.

## Communicatieadvies

Wij adviseren de organisatie om volgens de onderstaande communicatiematrix te communiceren.

[Kruis aan wie welke informatie moet gaan krijgen.]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Gevonden zwakheden | Beschrijving gevonden bewijzen | Inhoudelijk gevonden bewijzen | Aangebrachte aanpassingen | Bericht mogelijk datalek |
| Jouw leidinggevende | x | x | x | x | x |
| Securityofficer van AmeRijck | x | x | x | x | x |
| Directie van AmeRijck | x | x | x | x | x |
| Lokale media |  |  |  |  |  |
| Nationale media |  |  |  |  |  |
| Meldloket datalekken | x |  |  |  |  |
| Politie |  |  |  |  |  |
| De afdeling IT van AmeRijck |  |  |  |  |  |
| De afdeling Marketing van AmeRijck |  |  |  |  |  |
| De receptie van AmeRijck |  |  |  |  |  |

[NB Gebruik gerust het internet, maar vermeld wel een gevonden bron en beschrijf altijd de gevonden informatie in eigen woorden.]