# Bijlage 2.1 Sjabloon onderzoeksverslag

Datum 18-4-2023

Auteur Yadon Refos

## Opdrachtgever

Securityofficer AmeRijck vakantiepark

## Managementsamenvatting

Bij de apotheek Amerijck hebben zij een grote datalek daar gaat de directie ervan uit. De datalek via de databaseserver is gebeurt. Er is een remote accesstool gedownload en actief zodat ik kan zien of er een ongecontroleerde wijze toegang kan worden verkregen tot de databaseserver. Het rootwachtwoord van MySQL is root hierdoor kan elke medewerker de databaseserver in.

Ik moet ook uitzoeken hoe het is gebeurt en de acties verwerken in de praktijk.

## Overzicht onderzoek

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

Er werd onderzocht via de zwakheden die werden genoteerd moest ik kijken hoe het werd ontstaan zodat ik het later kan verwerken in de praktijk.

### Wat is er onderzocht?

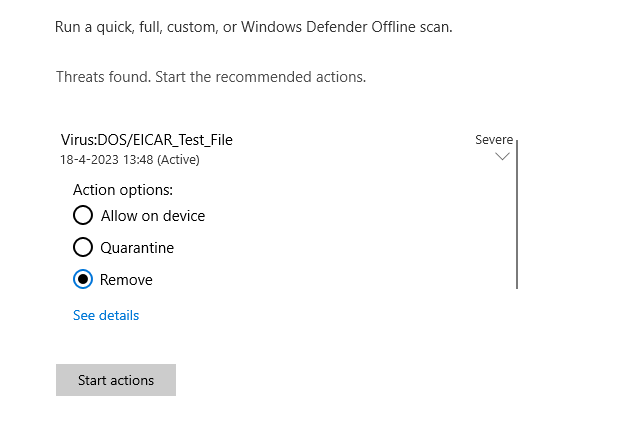
[Een beschrijving van de punten waarop controles zijn uitgevoerd.]

We moesten via de remote accesstool, MySQL, de firewall en via de antivirusbescherming kijken.

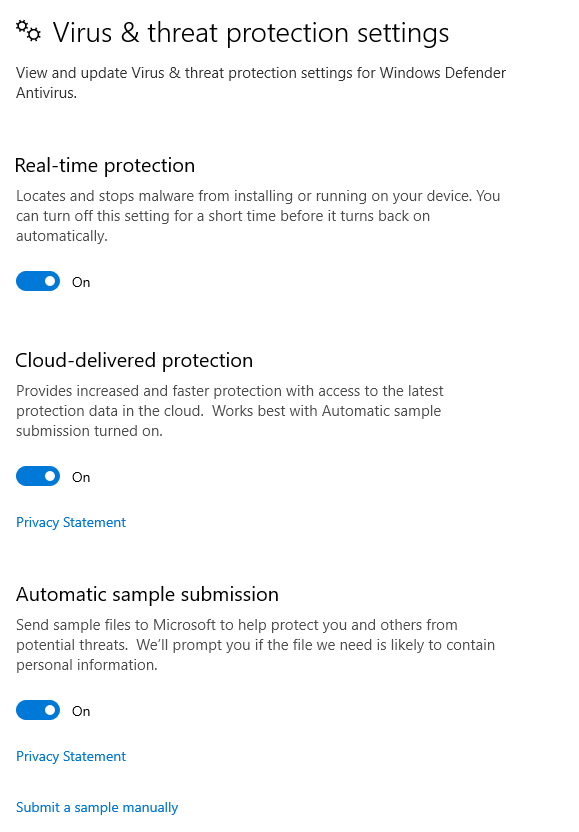
Van Joeman mag ik de Firewall scan niet uitvoeren vanwege complicaties.

### Gevonden zwakheden

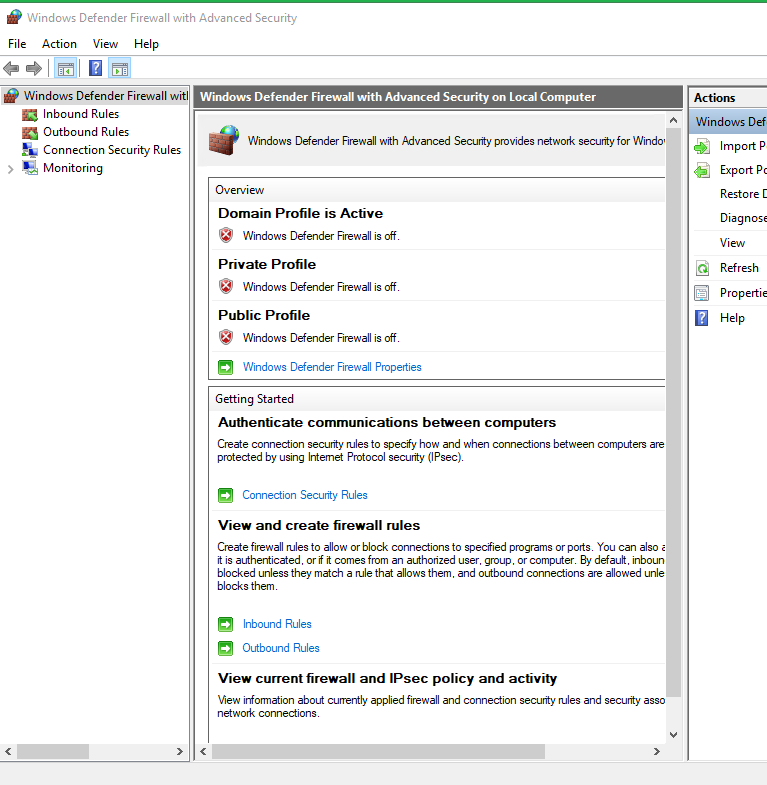
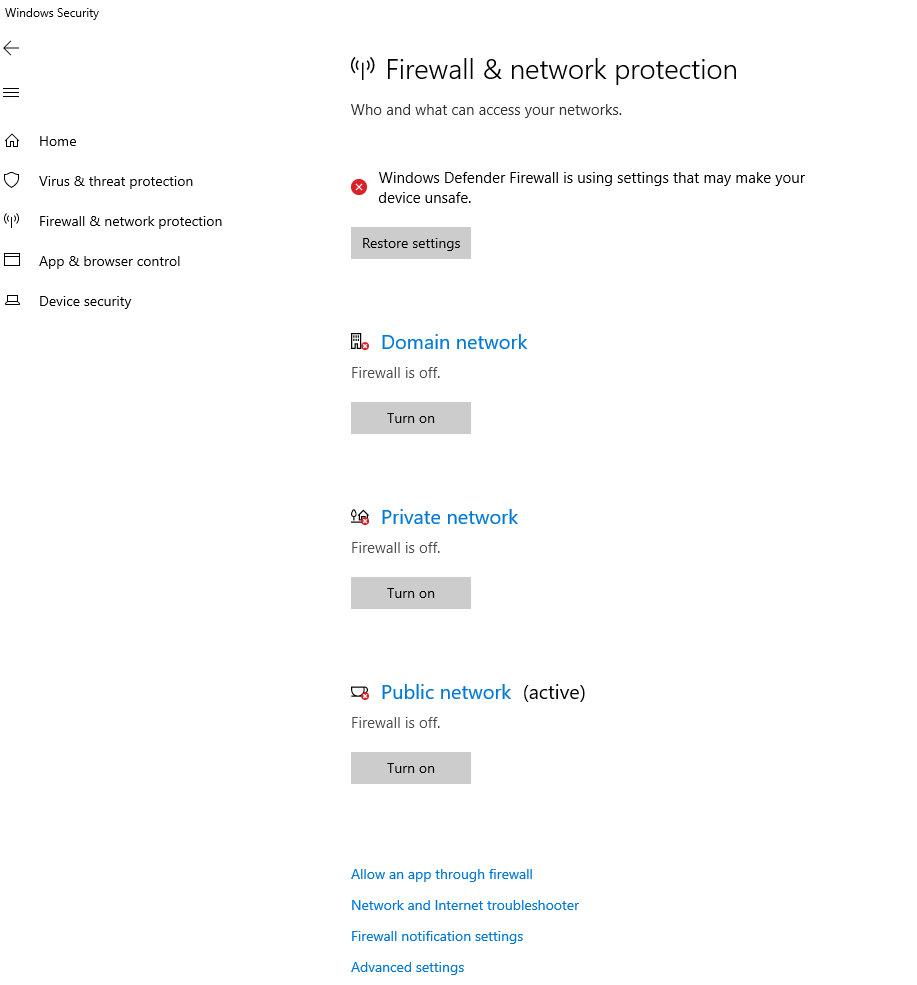
[Beschrijf de zwakheden met hun risiconiveau die mogelijk hebben bijgedragen tot het incident. Gebruik eventueel de matrix om dit overzichtelijk te rapporteren.]



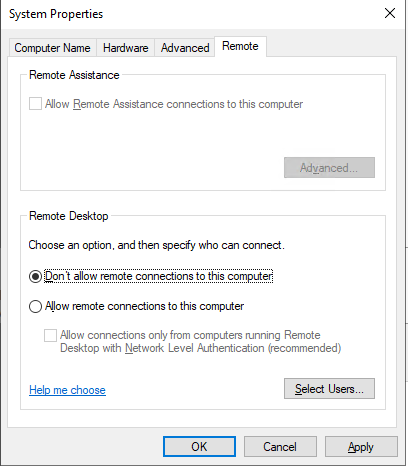
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Kans 🡺 | Risicomatrix | | | |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Impact 🡺 | | | |
| Kans is groot |  | | | |
| Impact | De gevolgen van geen Full scan is dat u kwetsbaar bent voor gevaren van buitenaf zo kunnen cybercriminelen makkelijk binnen uw systeem komen en ze kun gevaarlijke bestanden versturen zodat ze controle van uw pc kunnen krijgen. | | | |
|  |  | | | |
|  |  | | | |



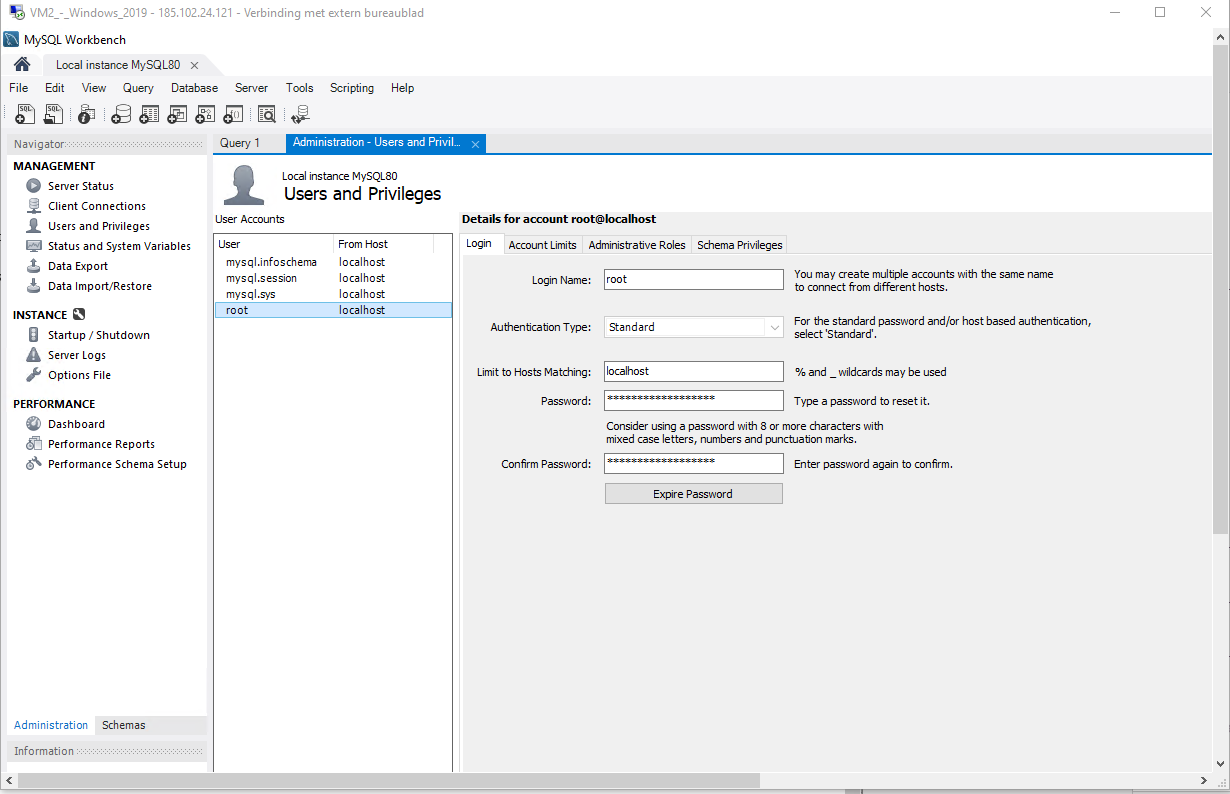
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Kans 🡺 | Risicomatrix | | | |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Impact 🡺 | | | |
| Kans is groot |  | | | |
| Impact | Als de virus & Threat niet aan staat kunnen er gevaarlijke virussen en spyware binnen jouw pc komen het advies is om het altijd te scannen. Mijn advies is dat er om de maand een check wordt gedaan | | | |



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Kans 🡺 | Risicomatrix | | | |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Impact 🡺 de firewall mag niet aan omdat de docent Joeman het zij vanwege complicaties | | | |
| Kans is groot |  | | | |
| Impact |  | | | |



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Kans 🡺 | Risicomatrix | | | |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Impact 🡺 het gevolg hiervan is dat iedereen beschikking heeft tot elke map. Advies is niet elke gebruiker moet recht hebben op het systeem. Elke gebruiker moet bepaalde rechten hebben. | | | |
| Kans is groot |  | | | |
| Impact |  | | | |



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Kans 🡺 | Risicomatrix | | | |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Impact 🡺 het gevolg hiervan is dat iedereen toegang heeft tot SQL workbench. Mijn advies is dat het wachtwoord om 2 maanden aangepast moet worden. | | | |
| Kans is groot |  | | | |
| Impact |  | | | |

### Beschrijving gevonden bewijzen van eventueel misbruik

[Beschrijf welk *soort* bewijzen zijn gevonden.]

### Inhoud van gevonden bewijzen

[Beschrijf de relevante details van de bewijzen.]

### 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.]

## Conclusie

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

## Advies

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

## 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 |  |  |  |  |
| Securityofficer van AmeRijck | x | x |  |  | x |
| Directie van AmeRijck |  |  | x |  |  |
| Lokale media | x |  |  |  |  |
| Nationale media |  |  | x |  |  |
| Meldloket datalekken | x |  |  |  | x |
| Politie | x |  |  |  |  |
| De afdeling IT van AmeRijck | x |  | x |  |  |
| De afdeling Marketing van AmeRijck | x |  |  | x |  |
| De receptie van AmeRijck | x |  |  | x |  |

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