# Bijlage 2.1 Sjabloon onderzoeksverslag

Datum 4-6-2025

Auteur Shaylandro Amatkarijo

## Opdrachtgever

Securityofficer AmeRijck vakantiepark

## Managementsamenvatting

Ik heb de firewall, antivirusbescherming, virusinfectie en of er een remote accesstool is geïnstalleerd gecheckt. Aan de hand van de local server tab kon ik al zien dat de firewall en de antivirusbescherming uit staan en die heb ik weer aangezet. Hou die voortaan aan. Ik heb een scan voor de virusinfectie gedaan en er was geen virus. Ik heb via event viewer gecheckt of er een remote accesstool is geïnstalleerd.

## Overzicht onderzoek

Ik heb de firewall, antivirusbescherming, virusinfectie en of er een remote accesstool is geïnstalleerd gecheckt. Aan de hand van de local server tab kon ik al zien dat de firewall en de antivirusbescherming uit staan. Ik heb een scan voor de virusinfectie gedaan en er was geen virus. Ik heb via event viewer gecheckt of er een remote accesstool is geïnstalleerd.

### Wat is er onderzocht?

Ik heb gecheckt op de firewall en de antivirusbescherming uit staan, ze stonden idd uit en ik heb ze weer aangezet. Ook heb ik onderzocht of er een virusinfectie is door een scan te doen, waaruit blijkt dat er geen virusinfectie is. Ik heb in de event viewer gecheckt of er een remote accesstool is geïnstalleerd, waaruit blijkt dat het ook echt geïnstalleerd.

### 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 | | | |
| De firewall is uitgezet | Er is geen strong authentication afgedwongen in de database. | Een remote accesstool is geïnstalleerd en actief waardoor er op ongecontroleerde wijze toegang verkregen ka worden tot de database server. |  |
|  | De antivirusbescherming is uitgezet. | Het rootpassword van MySQL is ‘root’. Hierdoor kan in feite iedereen die op de databaseserver is ingelogd, rootaccess krijgen tot de database. |  |
|  |  | Er is een virusinfectie. |  |
| Impact 🡺 | | | |

### Beschrijving gevonden bewijzen van eventueel misbruik

Aan de hand van de screenshots zijn de bewijzen.

### Inhoud van gevonden bewijzen

[Beschrijf de relevante details van de bewijzen.]

### Bericht mogelijk datalek

Er moet een melding gedaan worden bij het meldloket, want er is op een ongecontroleerde wijze een remote accesstool geïnstalleerd terwijl de firewall en het antivirusbescherming uit stonden.

## Conclusie

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

## Advies

Hou de firewall en het antivirusbescherming aan zodat er niet op een ongecontroleerde wijze een remote accesstool kan worden geïnstalleerd

## 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 | Firewall en antivirusbescherming stonden uit waardoor er een remote accesstool is geïnstalleerd | Aan de hand van de screenshots te zien | Firewall en antivirusbescherming aangezet |  |
| Securityofficer van AmeRijck | x | Firewall en antivirusbescherming stonden uit waardoor er een remote accesstool is geïnstalleerd | Aan de hand van de screenshots te zien | Firewall en antivirusbescherming aangezet |  |
| Directie van AmeRijck |  |  |  |  |  |
| Lokale media |  |  |  |  |  |
| Nationale media |  |  |  |  |  |
| Meldloket datalekken | x | Firewall en antivirusbescherming stonden uit waardoor er een remote accesstool is geïnstalleerd | Aan de hand van de screenshots te zien | Firewall en antivirusbescherming aangezet |  |
| Politie |  |  |  |  |  |
| De afdeling IT van AmeRijck | x | Firewall en antivirusbescherming stonden uit waardoor er een remote accesstool is geïnstalleerd | Aan de hand van de screenshots te zien | Firewall en antivirusbescherming aangezet |  |
| 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.]

















