Bijlage 2.1 Sjabloon onderzoeksverslag

Datum

Auteur

**Opdrachtgever**

Securityofficer AmeRijck vakantiepark

**Managementsamenvatting**

Wij begonnen eerst met het bestuderen van de instellingen we keken naar de zaken als updates,

automatische updates, staat de firewall aan en naar de open poorten. Vervolgens gingen we alle

zaken die niet horen rechtzetten.

**Overzicht onderzoek**

De SRV002 draait MYSQL server met een apothekersdatabase waarin informatie is opgeslagen van de

gasten. Op een forum is informatie gevonden van de gasten dat duidelijk een informatie lek

aangeeft. Wij hebben onderzocht wat de computer zo kwetsbaar maakt vervolgens zijn we in mysql

gaan kijken.

**Wat is er onderzocht?**

Alles wat wij hebben onderzocht is.

- Of er een virus is en hoe die binnen is gekomen.

- Een data lek

**Gevonden zwakheden**

Wij hebben een virus vastgesteld en verwijderd.

De database had een hele makkelijke wachtwoord genaamd “root” die is gewijzigd naar:

MNFK98Oamerijck.

Afbeelding met tekst, schermopname, visitekaartje, Lettertype

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, Lettertype, lijn

Automatisch gegenereerde beschrijving

Afwijking 1: Iedereen rechten geven tot de server

Impact: Als iemand toegang tot de server heeft zou je tot alle bestanden kunnen komen maar nog

niet in de database die heeft een andere wachtwoord nodig.

Afwijking 2: Wachtwoord nooit gewijzigd van mysql database. Als een vreemdeling toegang heeft tot

de Database zou die persoon overal in kunnen komen en ook tot gevoelige informatie van klanten.

Afwijking 3: iedereen moet zijn wachtwoord wijzigen en goed beveiligen

Afwijking 4: Automatic updates aanzetten: zorg ervoor dat je apparaten up to date zijn

Afwijking 5: zet firewall aan dat zorgt ervoor dat er minder snel virussen komen

Afwijking 6: iedreen moet zijn wachtwoorden om de 2 maanden wijzigen zodat hackers moeilijker

wachtwoorden kraken

Afwijking 7

Beschrijving gevonden bewijzen van eventueel misbruik

Hier zou een login zijn geweest wat er niet heel veilig uit ziet. Er is hier door iemand ingelogd maar

het is niet te zien door wie.

Afbeelding met tekst, schermopname, Lettertype, lijn

Automatisch gegenereerde beschrijving

**Inhoud van gevonden bewijzen**

Iemand probeerde in te loggen maar het is niet gelukt.

**Bericht mogelijk datalek**

**Conclusie**

Mijn conclusie is dat het er veel meer aan beveiliging besteed moet worden want er is niks op het

gebied van beveiliging gedaan. Heel veel poorten staan open, het is niet duidelijk wie toegang heeft

tot de database en wie bepaalde rechten heeft.

**Advies**

Bijlage 2.1 Sjabloon Onderzoeksverslag - EX\_IT20\_EP8\_P2-K2\_1v1 4/3

Mijn advies is dat niet elke gebruiker evenveel rechten heeft om in de server te komen. Elke

gebruiker moet bepaalde rechten hebben. De wachtwoorden moeten om de 2 maanden gewijzigd

worden van elke gebruiker. Automatische updates op bepaalde tijdstippen aanzetten. Elke apparaat

up to date houden. Mijn laatste advies is dat de firewall aangezet moet worden.

Afbeelding met tekst, nummer, schermopname, Lettertype

Automatisch gegenereerde beschrijving

Afbeelding met tekst, schermopname, brief, Lettertype

Automatisch gegenereerde beschrijving

**Bijlage 2.3 Zwakheden**

In het onderstaande worden de zwakheden benoemd die in ieder geval op SRV002 gevonden kunnen

worden en mogelijk hebben bijgedragen aan het datalek.

**Zwakheden SRV002**

 Een remote accesstool is geïnstalleerd en actief waardoor er op ongecontroleerde wijze

toegang verkregen kan worden tot de databaseserver.

 Het rootpassword van MySQL is ‘root’. Hierdoor kan in feite iedereen die op de

databaseserver is ingelogd, rootaccess krijgen tot de database.

 Er is geen strong authentication afgedwongen in de database.

 De firewall is uitgezet.

 De antivirusbescherming is uitgezet.

 Er is een virusinfectie.

**Logboek**

**Datum:4-06-2023**

**Auteur: Reh**

**Afbeelding met tekst, schermopname, software, Webpagina

Automatisch gegenereerde beschrijving**

**Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving**

**Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving**

**Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving**

**Afbeelding met schermopname, tekst

Automatisch gegenereerde beschrijving**

**Afbeelding met tekst, schermopname, software, nummer

Automatisch gegenereerde beschrijving**

**Afbeelding met tekst, software, Webpagina, Computerpictogram

Automatisch gegenereerde beschrijving**

**Afbeelding met tekst, schermopname, Lettertype, nummer

Automatisch gegenereerde beschrijving**

Afbeelding met tekst, schermopname, Lettertype

Automatisch gegenereerde beschrijving