Bijlage 4.1 Logboek onderzoek conclusies en samenvatting

Let op: De antwoordvelden worden groter als er geen ruimte meer is. Het gebruik van screenshots ook in de antwoordvelden plaatsen.

|  |
| --- |
| * *Overzicht hele onderzoek: Hier leg je uit wat je allemaal onderzocht hebt* |
| In dit onderzoek is het logbestand van een FTP-server geanalyseerd. Het doel was om verdachte activiteiten te indentificeren, zoals ongeautoriseerde toegang, mislukte inlogpogingen en overdracht van gevoelige bestanden. |
| * *Gedetailleerde resultaten: Hier stel je vast wat je gevonden hebt op detail niveau (Denk hierbij aan IP, Port, Users, Time, Data)* |
| **Gebruikers:** BramBurg en AnnieStryker  **IP – addressen:** 10.0.191.12, 10.101.0.77 en 150.151.12.1  **Tijdstempels:** Activiteiten tussen 2023-01-09T05:12:32 en 2023-01-09-T14:16:32  **Bestanden gedownload:** Nacha File.xlsx, FY20 Budget template\_V1\_1105\_April update.xlsx , Fee Income 2021\_October.pdf , FY21 Rent-Security Deposits.xlsx , Loan-Forgiveness-Calculation-Workbook from Valley.xlsx  **Verdachte activiteiten:** Meerdere mislukte inlogpogingen van gebruiker AnnieStryker , Herhaalde toegang tot gevoelige mappen zoals `/Data/Accounting\_safe`   en Download van gevoelige financiële documenten |
| * *Conclusie: Maak een conclusie op basis van je bevindingen* |
| De logs tonen aan dat er meerdere pogingen zijn gedaan om in te loggen met verkeerde wachtwoorden. Uiteindelijk is toegang verkregen tot gevoelige bestanden. Dit wijst op een mogelijk beveiligingsincident. |
| * *Advies: Geef advies op basis van je conclusie* |
| Verander direct alle wachtwoorden  Beperk toegang tot gevoelige mappen  Implementeer 2FA  Monitor netwerkverkeer op verdachte patronen  Overweeg forensisch onderzoek |
| * *Communicatieadvies: Wie moeten hier allemaal van op de hoogte gebracht zijn? (Denk ook aan AVG!)* |
| Informeren:  IT-beveiligingsteam  Directie  Functionaris Gegevensbescherming(AVG)  Betrokken medewerkers |
| * *Managementsamenvatting: Geef een samenvatting voor de directie, let hierbij weer op jargon.* |
| Uit het onderzoek blijk dat een gebruiker meerdere keren heeft geprobeerd in te loggen op de FTP-server en uiteindelijk toegang heeft gekregen tot gevoelige documenten. Er is sprake van een mogelijk datalek. Directie actie is vereist om verdere schade te verkomen. |