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* |
| Ik heb een logbestand onderzocht van een FTP-server (bestanden delen via internet). Ik heb gekeken welke gebruikers inlogden, welke apparaten/IP-adressen werden gebruikt, welke bestanden zijn bekeken of gedownload, en of er fouten of verdachte activiteiten waren. |
| * *Gedetailleerde resultaten: Hier stel je vast wat je gevonden hebt op detail niveau (Denk hierbij aan IP, Port, Users, Time, Data)* |
| * **Gebruikers:**   + *BramBurg*: meerdere succesvolle logins.   + *AnnieStryker*: eerst mislukte logins, daarna succesvol. * **IP-adressen:**   + 10.0.191.12 en 10.101.0.77 (interne IP’s),   + 150.151.12.1 (mogelijk extern, bijv. via VPN). * **Tijd:**   + Activiteit op 9 januari 2023 van 05:12 tot 14:16. * **Bestanden:**   + o.a. “Nacha File.xlsx”, “FY20 Budget template”, “Fee Income.pdf”, “Loan Forgiveness.xlsx”. * **Fouten:**   + Login foutmeldingen (530 Login incorrect).   + Time-outs (421 No-transfer-time exceeded). |
| * *Conclusie: Maak een conclusie op basis van je bevindingen* |
| De server wordt actief gebruikt door bekende gebruikers. Sommige verbindingen komen van mogelijk externe netwerken. Er zijn foutmeldingen en time-outs, maar geen bewijs van een aanval. Wel zijn er verbeteringen nodig in de beveiliging. |
| * *Advies: Geef advies op basis van je conclusie* |
| * Sta alleen bekende IP-adressen toe. * Gebruik veilige verbindingen zoals SFTP of FTPS. * Stel limieten in bij foute inlogpogingen. * Monitor toegang vanaf externe netwerken. |
| * *Communicatieadvies: Wie moeten hier allemaal van op de hoogte gebracht zijn? (Denk ook aan AVG!)* |
|  IT-beheerteam   Privacy Officer (AVG-verantwoordelijke)   Gebruikers BramBurg en AnnieStryker   Eventueel de netwerkbeveiligingsverantwoordelijke |
| * *Managementsamenvatting: Geef een samenvatting voor de directie, let hierbij weer op jargon.* |
| Tijdens onderzoek naar het FTP-verkeer zijn geen directe bedreigingen vastgesteld. Wel zijn er kwetsbaarheden geconstateerd, zoals onbeveiligde externe toegangspogingen en gebrekkige wachtwoordbeveiliging. Advies: verhoog de netwerkveiligheid en versleutel dataverkeer om compliance en risicovermindering te waarborgen. |