Cybersecurity Assessment Report voor Bike Mobile

Dit rapport geeft een volledig beeld van de uitgevoerde cybersecurity assessment uitgevoerd in naam van Bike Mobile. In dit rapport staan onze bevindingen van zowel de externe scan van buiten het netwerk (black box) als de interne netwerk scan (white box).

Uit ons onderzoek zijn een aantal kritieke items gekomen die direct aangepakt moeten worden na het opleveren en doorlezen van dit rapport. Tevens hebben we in dit rapport een aantal aan te raden acties staan om ervoor te zorgen dat er geen herhalingen plaats vinden van onze bevindingen. Bij elke bevinding staat hoe kritiek de bevinding is, van Low naar Critical.

In de volgende delen staan onze bevindingen uitgelijnd en waarom deze van belang zijn voor de lange termijn beveiliging van Bike Mobile

Black Box Scan Summary voor Bike Mobile:

De black box scan van de webserver en de database server heeft ons inzicht gegeven in een aantal kritieke problemen met de infrastructuur van het bedrijf:

- **Anonymous FTP Access (Critical)**: De FTP Service is ingesteld om anoniem inloggen toe te staan. Dit betekent dat iedereen die weet hoe FTP werkt in kan loggen op de ftp-server en heeft hiermee toegang tot alle bestanden in de WWW folder. Hoewel de bestands rechten goed genoeg ingesteld zijn dat uploaden zonder de correcte login niet mogelijk is kan de anonieme gebruiker wel bestanden inzien en downloaden. Dit maakt de kans op data lekken heel groot.

- **Outdated Apache Version (Low)**: De webserver draait op het moment van de scan op Apache versie 2.5.25. Dit is niet de meest recente versie en omdat Apache met regelmaat bekenede lekken dichtmaakt is het aan te raden om altijd op de laatste stabiele versie van Apache te draaien.

- **HTTP Security Headers (Medium)**: Het gebrek aan http-security headers, zoals “X-Frame-Options" en “X-Content-Type-Options", dit houdt de site open voor aanvallen als “clickjacking” en “MIME type sniffing”.

- **MySQL Accounts Without Passwords (Critical)**: Tijdens de black box scan kregen we de impressie dat de accounts die gebruikt worden om toegang te krijgen tot de MySQL database geen wachtwoorden hebben. Meer hierover bij de White box scan.
- **PHP Configuration Lapses (Medium)**: De variabele “**open_basedir”** is niet ingesteld, wat de optie openzet om PHP-scripts te kunnen uitvoeren en toegang te

krijgen tot bestanden buiten de WWW folder. Tevens is het **info.php** bestand toegankelijk op de website. Het uitvoeren van dit bestand laat heel veel systeem informatie zien die gebruikt kan worden om andere aanvallen uit te voeren.

- **Unnecessary Open Ports (Low)**: Poort 2000 en 5060 staan open zonder dat de nodige services aanwezig zijn. Deze poorten worden vaak gebruikt voor VoIP maar dit kunnen wij niet als aanwezig detecteren dus staan deze poorten onnodig open. Dit geeft aanvallers een extra mogelijkheid om binnen te kunnen komen.

- **SSL/TLS Encryption Not Detected (Medium)**: Er is geen SSL of TLS gevonden op de website. Hoewel dit tijdens development geen probleem is, is het sterk aan te raden dit op de productie omgeving wel door te voeren als extra laag beveiliging. Dit zodat persoonlijke data van klanten altijd die extra laag heeft.

Alle bevindingen hierboven kunnen gebruikt worden door aanvallers om binnen te komen binnen het netwerk en is dus een mogelijkheid voor de netwerk en data integriteit van Bike Mobile. De afwezigheid van basis beveiligings items zoals SSL en het anoniem in kunnen loggen op de FTP Server geeft aan dat direct actie moet worden ondernomen.

White Box Scan Summary voor Bike Mobile:

De white box scan heeft een aantal kritieke punten van interesse aan het licht gebracht:

- **MariaDB Root Access (Low)**: De MariaDB database staat toe dat van buiten het interne netwerk er met de root gebruiker ingelogd kan worden. Hoewel dit niet op

zichzelf een probleem is kan een aanvaller hier wel misbruik van maken als hij het wachtwoord weet te achterhalen.

- **SSH Root Login Enabled (Low)**: De SSH service heeft ook root login aanstaan. Net zoals voor MariaDB is dit niet op zichzelf een probleem maar het kan een groot probleem worden als iemand het wachtwoord weet te achterhalen gezien diegene hiermee de hele webserver onder controle kan nemen.

- **No SSL/TLS on Web Server (Medium)**: Er is geen SSL/TLS aanwezig op de webserver. Dit geeft aan dat alle data inclusief wachtwoorden en andere gebruikers data in plain tekst naar de server gezonden wordt. Dit maakt het heel makkelijk voor een aanvaller om mee te lezen met alles wat er tussen de gebruiker en de server verzonden wordt.

- **Unnecessary Open Ports (Medium)**: Zoals we tijdens de black box scan dachten blijkt tijdens de white box scan dat er inderdaad geen VoIP service aanwezig is en dit betekent dus dat de poorten 2000 en 5060 onnodig open staan, wat aanvallers een onnodige extra mogelijkheid geeft om binnen te kunnen komen.

- **Discrepancy in OS Versions (Low)**: Tijdens de scan zijn we erachter gekomen dat de webserver draait om Debian 9 en de database server draait op Debian 10. Hoewel dit geen probleem is, is het aan te raden beide server minimaal op Debian 10 te hebben zodat ze op dezelfde OS-versie zitten en het liefst te upgraden naar Debian 11. Dit om te voorkomen dat bekende problemen met oude Debian versies gebruikt kunnen worden.

Index.php Plain Text Credentials (Critical):

- Het bestand **index.php** bevat een wachtwoord en gebruikersnaam in te lezen tekst. Omdat tijdens de white box scan is gebleken dat dit wachtwoord hetzelfde wachtwoord is wat gebruikt wordt op alle servers en services betekent dit dat elk systeem binnen het netwerk nu op in te loggen valt. Dit omdat het root account toegang geeft tot alle functies binnen een OS.

Immediate Actions Post-Audit voor Bike Mobile:

Na aflevering van dit rapport raden wij Bike Mobile streng aan om de acties hieronder aangegeven uit te voeren, om direct de grootste beveiligings lekken te dichten.

- **Password Reset and Policy Enforcement**: Verander direct het masterwachtwoord wat bekend gemaakt is in **index.php**. Stel hier een nieuw robuust wachtwoord voor in en zorg ervoor dat op termijn alle servers en services hun eigen unieke wachtwoord krijgen.

- **Secure Database Configuration**: Zet root toegang tot de database uit voor externe toegang. Dit om te voorkomen dat er toegang van buitenaf mogelijk is.

- **Implement SSL/TLS**: Zorg ervoor dat er een SSL-certificaat aan de webserver gekoppeld wordt zodat alle data die van en naar de server gestuurd wordt veilig is.

- **Close Unnecessary Ports**: Sluit de poorten 2000 en 5060 voor externe toegang, gezien er geen diensten actief zijn die deze poorten nodig zijn. Kijk ook nog kritisch naar de andere open poorten en of deze nodig zijn.

- **FTP Service Encryption**: Vervang de ftp-service naar FTPS of SFTP om bestands overdracht veilig te houden. Tevens moet anonieme login direct uitgezet worden om te voorkomen dat mensen bij de server bestanden kunnen.

- **VPN-Only Access**: Maak een VPN-verbinding mogelijk voor toegang tot SSH, FTP en databasemanagement. Dit zodat deze verbindingen niet direct aan het internet open staan en daardoor wordt de kans dat een aanvaller hier wat mee kan aanzienlijk kleiner.

- **Remove Sensitive Information**: Verwijder direct de login gegevens uit de code van **index.php**. Vervang deze met een beveiligde methode die niet de login gegevens direct laat zien.

Ter conclusie, dit document heeft de problemen met de netwerk setup en beveiliging van Bike Mobile aan het licht gebracht. Wij hopen door middel van dit rapport dat Bike Mobile genoeg op weg te helpen om de nu bekende problemen op te kunnen lossen.

Dit rapport markeert het einde van de huidige audit, en we kijken uit naar de voortgang van Bike Mobile's netwerk en beveiliging gebaseerd op de bevindingen in dit rapport.