|  |  |
| --- | --- |
| **Angriffsbeschreibung** | |
| **Name:** Zugriffsverletzung WLAN | **Hauptverantwortlicher**: Simeon Weigel |
| **Ziel des Angriffs**: Zugang zum fremden WLAN | **Gefährdete Personengruppen**: Alle |
| **Beispiel eines Angriffsszenarios** | |
| Akteure : Frau Müller , Herr Zimmermann **Fallbeschreibung**:  Frau Müller möchte ihren alten USB-Stick auf eBay verkaufen. Aus Angst, das jemand ihre persönlichen Daten lesen kann, löscht Sie ihre Daten. (Exemplarisch eine *Textdatei*: LoginnamePasswort). | |
| *1 . Ausgangssituation:* | |

Ein Bild, das Screenshot enthält.

Mit sehr hoher Zuverlässigkeit generierte Beschreibung

|  |
| --- |
| *2. Nach Löschen der Datei* |

Ein Bild, das Screenshot enthält.

Mit sehr hoher Zuverlässigkeit generierte Beschreibung

|  |
| --- |
| Frau Müller verkauft ihren USB-Stick an Herrn Zimmermann auf ebay. Herr Zimmermann hat böse Absichten und möchte sich den Daten von Frau Müller annehmen. Dazu verwendet er das Freewareprogramm *Recuva*, mit dem sich gelöschte Daten widerherstellen lassen. |
| *3. Widerherstellen der Datei mit Recuva* |

Ein Bild, das Screenshot enthält.

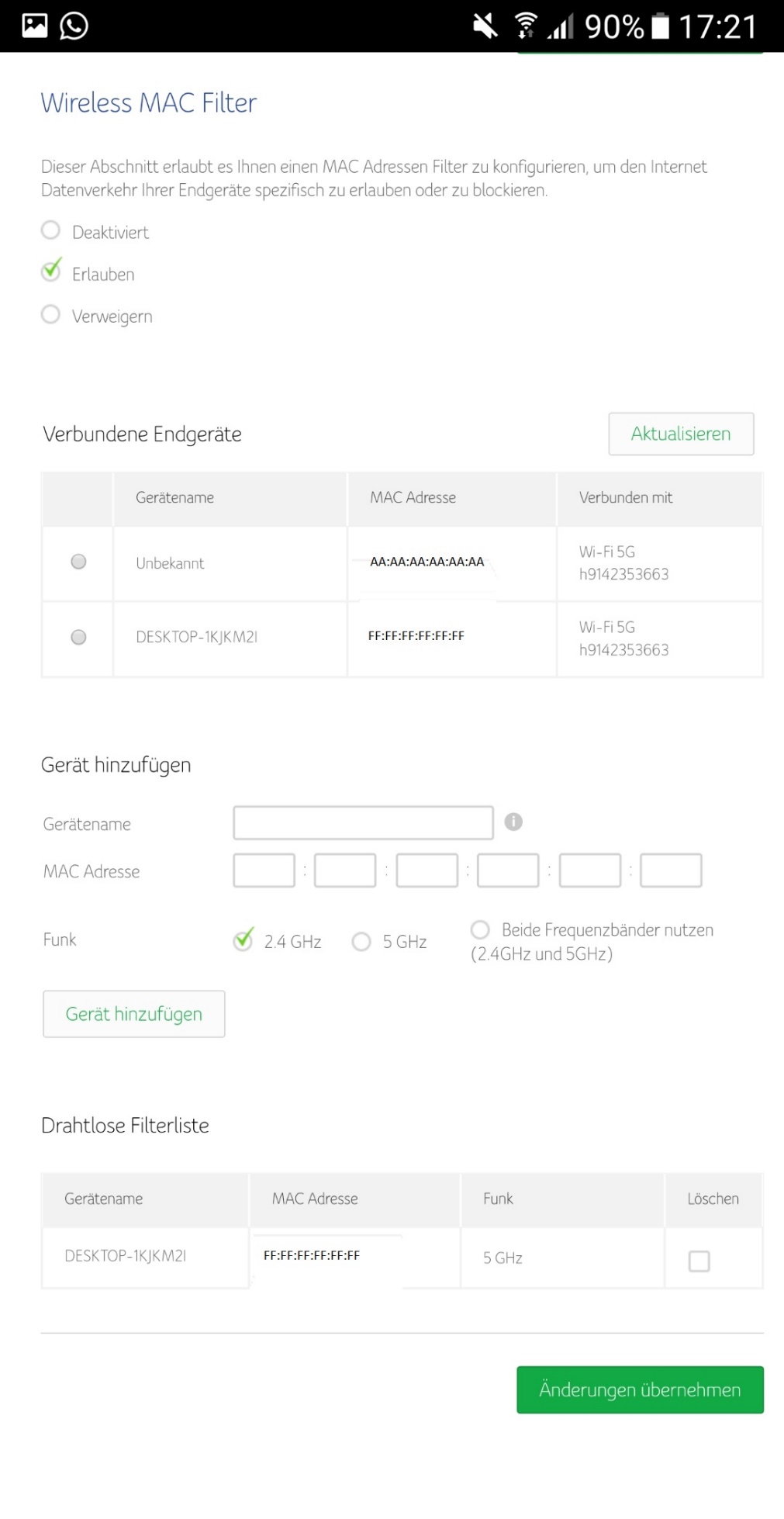
Mit sehr hoher Zuverlässigkeit generierte Beschreibung

|  |
| --- |
| *4. Inhalt der Datei nach Widerherstellung* |

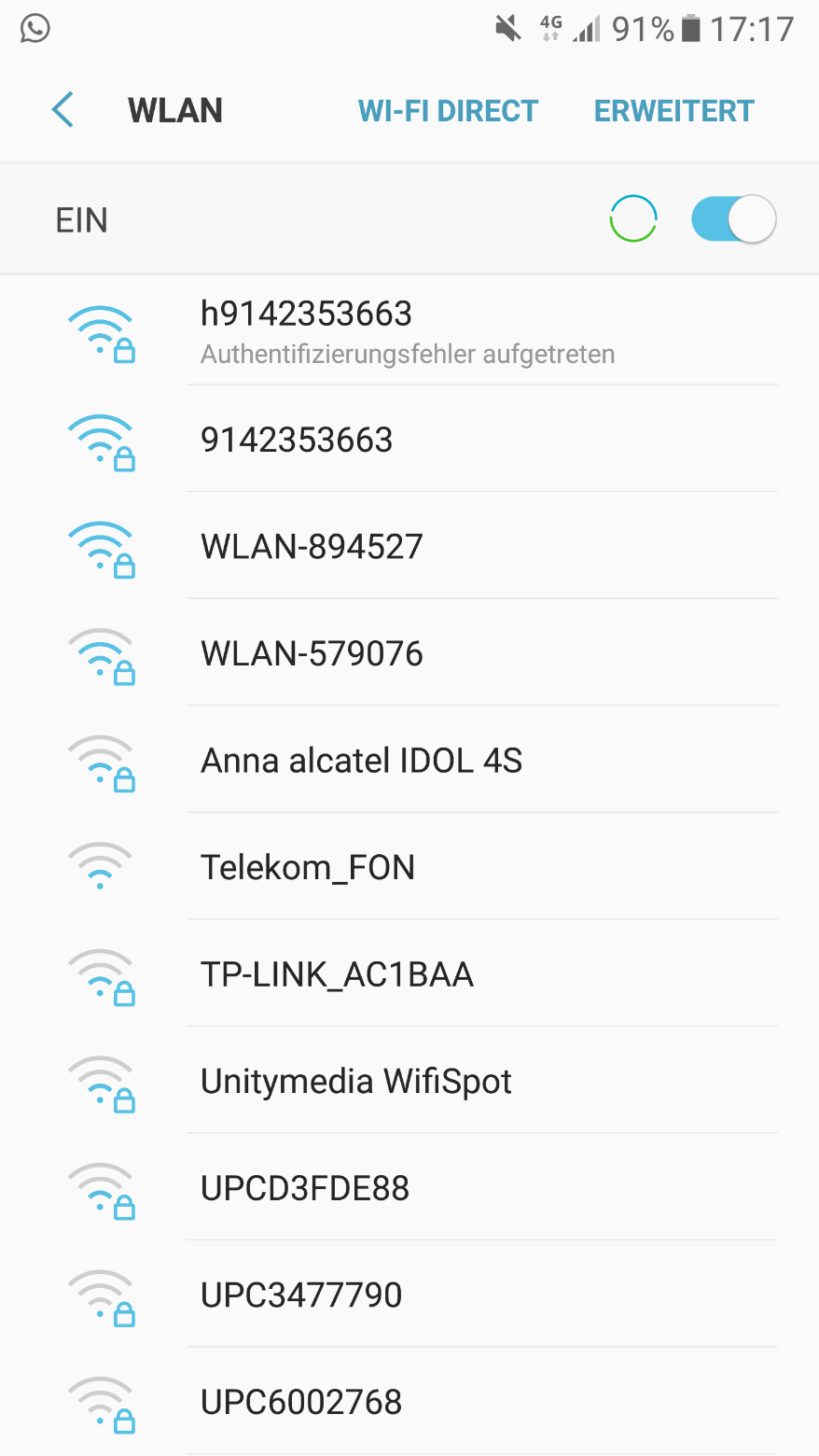
Ein Bild, das Screenshot enthält.

Mit sehr hoher Zuverlässigkeit generierte Beschreibung

|  |
| --- |
| Der Angreifer kann nun alle vertrauliche Daten von Frau Müller einsehen. |
| **Kommentare**: Ein mögliches Szenario wäre zudem, das man seinen USB-Stick entsorgt und ein Angreifer sich diesen annimmt. |
| Schutzmaßnahmen |
| Um sein WLAN Netzwerk vor Angriffen vor Unbekannten zu schützen, sollte man die MAC-Filter-Funktion seines Routers aktivieren. So wäre dem Angreifer nicht mehr die Möglichkeit gegeben, ein Netzwerkpasswort zu Bruteforcen, da es unzulässigen MAC-Adressen unmöglich ist, sich überhaupt zu authentifizieren. |



|  |
| --- |
| *6. MAC-Adressenfilter-Funktion aktivieren* |



|  |
| --- |
| **Kommentare**:  Das Programm Abylon Shredder besitzt 5 verschiedene Sicherheitslevel:  0: normales Löschen – Verknüpfungen entfernen  1: 2x überschreiben mit binären Nullen  2: 3x überschreiben mit Nullen und Zufallszahlen  3: 7x überschreiben nach DoDII-Methode  4: 13x überschreiben DoDII und Zufallszahlen  5: 35x überschreiben (Peter Gutman Methode)  6:Für das Netzwerk ist nur ein Endgerät mit der MAC-Adresse von „DESKTOP-1KJKM2I“ erlaubt.  7:Jeder Verbindungsversuch zum Netzwerk „h9142353663“, wird mit unzulässiger MAC-Adresse blockiert.  Diese Möglichkeit schützt nicht davor, wenn man vertrauliche Daten in Dateinamen schreibt. |

Zusätzlich:

MAC-Adressen gibt es in 70 Billionen Kombinationen, somit ist es theoretisch möglich eine gültige Adresse zu erraten, um dann daraufhin das WLAN Passwort, ebenfalls zu Bruteforce‘n. Aber durch den Zeitaufwand der hier eine erhebliche Rolle spielt, wird die ganze Prozedur unattraktiv für den Angreifer.

Um die Sicherheit zu maximieren, besteht die Möglichkeit die Anzahl der Zugriffe auf den Router für je eine MAC-Adresse auf bestimmte Versuche pro Zeit zu beschränken. Ebenfalls sollte das WLAN-Zugangspasswort von Zeit zu Zeit geändert werden.