Allgemeines (Erläuterungen zu den Tabellen)

- Verschlüsselte Kommunikation:
  - Es wird aufgeführt, ob die stattfindende Kommunikation vollständig, teilweise oder nicht durch Verschlüsselung gesichert wird
  - Bei vollständiger Verschlüsselung kann der Inhalt der Kommunikation nicht direkt mitgelesen oder verändert werden
- Verschlüsselte Verbindungen abgesichert:
  - Umfasst die zusätzlichen Sicherheitsfunktionen, die eine Kompromittierung der Kommunikation, trotz angewendeter Verschlüsselung verhindern
  - SSH wurden nicht evaluiert und standardmäßig zugunsten des Produktes als sicher angenommen
- Aktive Authentifizierung:
  - Der Zugriff auf Funktionen zur Fernsteuerung oder Installation ist erst erlaubt nach Überprüfung der Nutzerberechtigung (bspw. durch Angabe Benutzername/Passwort)
- Manipulation durch Externe
  - Beschreibt die Möglichkeit eines unberechtigten Zugriffs auf Daten oder Funktionen der betrachteten Produkte
- Gesicherte Fernsteuerung
  - Gibt an ob und wie gut die Kommunikation bei einem Fernzugriff abgesichert wird

Almond+

Produkt	**Almond+**
Anbieter	**Securifi**
Getestete Komponenten und Software	Almond+ (FW Version AP2-R070-L009-W016-ZW016-ZB005) Smartphone App “Almond” 4.2
Verwendete Komponenten	Everspring On/Off Switch AN158-2
Enthaltene Schutzfunktionen	
Verschlüsselte Kommunikation	JA
Verschlüsselte Verbindungen abgesichert	JA
Aktive Authentifizierung	JA
Manipulation durch Externe	Keine Möglichkeit
Gesicherte Fernsteuerung	Wirksamer Schutz
Testergebnis	**Guter Schutz**
Erläuterung	Wirksames Schutzkonzept
Bemerkungen	Smartphone App überprüft Zertifikat selbst
Testzeitraum	Juni 2015
Getestet von	The Independent IT-Security Institute Magdeburg Germany

- Grundsätzlich gut gesichertes Produkt
- Implementiert sinnvolle Sicherheitsfeatures, wie bspw. zufällig generierte Zugangspasswörter und SSIDs nach Rücksetzung auf Werkseinstellungen
- Bietet keine Möglichkeit des lokalen Zugriffs über die App an; jegliche Fernsteuerung über die App geht über die Almond Server
- Erläuterung Schutzfunktionen:
    - Verschlüsselte Kommunikation:
        - Sämtliche Verbindungen nach außen sind über HTTPS (TLS 1.2) abgesichert
        - Ein Fallback auf das ältere und potentiell unsicherere TLS 1.0 wird verhindert
        - Fernzugriff über App ist ebenfalls über HTTPS abgesichert
        - Lediglich Zugriff auf lokale Webseite ist nicht gesichert
    - Aktive Authentifizierung:
        - Obligatorische Authentifizierung für Fernzugriff über App und Webportal (über Almond+ Account)
        - Möglichkeit der Pin-Sicherung des Basisgerätes selbst
- Testergebnis:
    - Realisiert insgesamt ein solides Sicherheitskonzept
    - Erste Android App im Test überhaupt, die selbst das verwendete Zertifikat überprüft und daher praktisch auch gegen Man-in-the-Middle-Angriffe absichert