Sicherheitstest: Codeatelier homee

Produkt	**homee**
Anbieter	**Codeatelier**
Getestete Komponenten und Software	homee Brain Cube, homee Z-Wave Cube, Smartphone App „Homee“
Verwendete Komponenten	Everspring On/Off Switch AN158-2
Enthaltene Schutzfunktionen	
Verschlüsselte Kommunikation	TEILWEISE
Verschlüsselte Verbindungen abgesichert	TEILWEISE
Aktive Authentifizierung	JA
Manipulation durch Externe	Anfällig für Manipulation
Gesicherte Fernsteuerung	Teilweise anfällig für Manipulation
Testergebnis	**Anfälliger Schutz**
Erläuterung	Kein Schutz gegen interne Angriffe
Bemerkungen	Lückenhafte Verschlüsselung spielt Angreifern in die Hände
Testzeitraum	Juli 2015
Getestet von	AV-TEST The Independent IT-Security Institute Magdeburg Germany

Bedeutung der in der Tabelle aufgeführten Punkte

Verschlüsselte Kommunikation
Es wird aufgeführt, ob die stattfindende Kommunikation vollständig, teilweise oder nicht durch Verschlüsselung gesichert wird. Bei einer vollständigen Verschlüsselung kann der Inhalt der Kommunikation nicht direkt mitgelesen oder verändert werden. Sind die Verbindungen nur teilweise verschlüsselt, so konnten sowohl verschlüsselte als auch nicht-verschlüsselte Verbindungen beobachtet werden.

Verschlüsselte Verbindungen abgesichert
Dieser Punkt umfasst die zusätzlichen Sicherheitsfunktionen, die eine Kompromittierung der Kommunikation, trotz angewendeter Verschlüsselung, verhindert. Dieser Punkt bezieht sich ausschließlich auf die verschlüsselten Verbindungen, alle anderen Verbindungen werden ignoriert.

Aktive Authentifizierung
Der Zugriff auf Funktionen zur Fernsteuerung oder Installation ist erst erlaubt, nach einer Überprüfung der Nutzerberechtigungen, beispielsweise durch Angabe von Benutzername und Passwort.

Manipulation durch Externe
Dies beschreibt die Möglichkeit eines unberechtigten Zugriffes auf Daten oder Funktionen der betrachteten Produkte von außen. Der Angreifer ist dabei nicht zwangsweise in das interne Netzwerk eingedrungen und greift das System so an, sondern kann dies potentiell auch außerhalb des internen Netzwerkes durchführen. Es umfasst sowohl das abfangen von Authentifizierungsdaten als auch die Manipulation ohne dieser Informationen. Es ist nicht auf den Fernzugriff begrenzt.

Gesicherte Fernsteuerung
Gibt an, ob und wie gut die Kommunikation bei einem Fernzugriff abgesichert wird. Dies beschränkt sich ausschließlich auf die Client-Seite des Fernzugriffs. Der Mitschnitt oder gar die Manipulation des Fernzugriff-Bestandteils der Basisstation ist für einen Angreifer aufwändiger und wird deshalb nur im Punkt „Manipulation durch Externe“ abgedeckt.