Steffen Wendzel: How to Increase the Security of Smart Buildings?

Der Autor erklärt zunächst die Rolle und Verbreitung von Smart Buildings in der Zukunft. Anschließend nennt er entscheidende Punkte die zu einer erhöhten Datensicherheit führen und erklärt diese ausführlich. Der erste Punkt ist die „Internet-Based Communication“ hier verweist der Autor auf Projekte der TU Vienna, die in den letzten Jahren verstärkt Protokolle verbessert und überarbeitet haben, wie z.B. BACnet und KNX. Laut ihren Aussagen hätte die Entwicklung bereits in den letzten 10 Jahren stattfinden müssen. Es geht hauptsächlich darum, die Protokolle die für die heutigen Anforderungen in Smart Homes nicht ausgelegt worden, nachzubessern. Sein Zweiter Punkt lautet: „Impact of Attacks“. Hier geht es darum das die Angriffe auf Smart Homes bisher nicht vollständig verstanden werden. Er unterscheidet aktive und passive Szenarios. Bei einem aktiven Szenario wird der Feueralarm ausgelöst und der Passagierverkehr kommt zum Erliegen. Bei einem passiven Szenario werden z.B. die Gesundheitsdaten auf dem Schwarzmarkt an Versicherungen verkauft. Er fasst am Ende zusammen, dass nur ein Übergeordneter und nicht nur technischer Schutz vor Angriffen gewährleistet sein muss damit ein Smart Home sicher sei. Als dritten Punkt spricht er über den Langzeit Support von Smart Homes. Es sei wichtig, so der Autor, das Smart Homes eine möglichkeit des Updatens bieten um langfristige Sicherheit zu gewährleisten. Auch bei der Hardware muss darauf geachtet werden. So müssen Systeme die auf die heutigen kryptographischen Standards optimiert sind, ebenfalls für später Standards die Rechenkapazitäten besitzen. Außerdem müssten Smart Home Netzwerke regelmäßig mit Sicherheitssoftware geprüft werden. Als vierten Punkt stellt er das „User-Oriented Software Design“ vor. So schreibt der Autor, dass selbst wenn die oberen Punkte gewährleistet sind das System so ausgelegt sein müsste das der Nutzer es tatsächlich auf dem neusten Stand hält. Hier wird auf FUSE-IT einem Projekt das sich auf die Entwicklung eines Nutzer freundlichen Sicherheitsdashboards spezialisiert hat. Als Fünften kritischen Punkt, sieht er die Implementierung der Network Stacks. Diese würden meist nur durch einen oder ein paar wenige Entwickler implementiert werden. Dies führe zu Sicherheitslücken. Als mögliche Lösung stellt er das BARNI vor. Dabei wird der Netzwerkverkehr gefiltert und Pakete die nicht den Sicherheitsstandards entsprechen blockiert. Dadurch werden unsicher Empfänger geschützt. Als letzten Punkt nennt der Autor den Zugang zu Sicherheitsstandards. Der Autor kritisiert das viele wichtige Standards nur unter Einschränkungen verfügbar sind z.B. durch Geldzahlungen. Freie Standard würden zu einem breiteren Einsatz führen.

Quelle:

Wendzel, Steffen. (2016). How to Increase the Security of Smart Buildings?. Communications of the ACM. 59. 47-49. 10.1145/2828636.

Thema: Einheitliche Standards – P3P

Das P3P-Projekt wurde 2002 vom WWW Konsortium als Standard für den Austausch von Datenschutzinformationen empfohlen.
Das P3P Projekt soll dem Nutzer helfen einen schnellen Überblick über die Nutzung von personenbezogenen Daten zu gewinnen. Das P3P konnte sich nicht durchsetzen.

Technik:

P3P kann kostenlos genutzt werden. Es basiert auf XML und es wird lediglich ein P3P Agent benötigt der kostenlos im Netz erhältlich ist. Hat der Nutzer den Agenten angelegt, kann er festlegen wie mit seinen Daten umgegangen werden soll. So kann der P3P Header die Informationen enthalten, welche Art von Daten erfasst werden, zu welchem Zweck diese erfasst werden, wie lange Sie gespeichert werden und wem Zugriff auf die Daten gegeben wird und welchen Gesetzen und Regeln die Datenverarbeitung gehorcht. Vor dem Besuch einer Webseite werden dann die Nutzerangaben mit den Webseitenangaben verglichen.

Quelle:
https://de.wikipedia.org/wiki/Platform_for_Privacy_Preferences_Project
(06.11.2017)