Allthings

Factsheet # 2

Sicherheitsstandards

Dieses Factsheet bietet einen Überblick zu den Sicherheitsmaßnahmen von Allthings zu den Themen Hosting, Datentransfer und Datenhaltung als auch Authentifizierung und Autorisierung.

Autor	Marco Lüthy
Rolle	Head of Engineering
Kontaktdaten	marco.luethy@allthings.me
Klassifizierung	Vertraulich
Version	05.06.2019

Hosting

Die folgenden Regulierungen beschreiben die Sicherheit der **Allthings** Hosting Umgebung:

- Die Webdienste laufen in ihrer eigenen privaten Cloud mit einem separaten öffentlichen und privaten Netzwerk.
- Alle Webdienste nutzen eine dynamische Lastenverteilung mit Autoskalierung um Lastspitzen aushalten zu können.
- Firewall Regeln limitieren den Zugriff auf die Cloud Dienste basierend auf IP- und Protokoll-basierten Regeln. HTTP und HTTPS sind die einzigen Protokolle, die aus dem öffentlichen Internet erreichbar sind.
- Alle Ressourcen werden in Echtzeit mit erweiterten Statustests überwacht, die nicht nur den Status der Instanzen messen, sondern auch Anwendungsfehler erfassen.
- Container Instanzen werden bei Ausfällen automatisch neu gestartet.
- Instanzen werden automatisch ersetzt, wenn ihre Statustests fehlschlagen.
- Das Hosting Datencenter erfüllt die Anforderungen an eine umfassende Liste von global Sicherheitsstandards, inklusive ISO 27001, PCI DSS Level 1, IT Grundschutz und die EU Datenschutz Direktive. Siehe auch AWS Cloud Compliance für weitere Informationen.

Datentransfer und Datenhaltung

Bezüglich Datentransfer und -haltung hat **Allthings** die folgenden Maßnahmen implementiert:

- Kundendaten werden in Irland gespeichert und verlassen niemals die EU.

Allthings

- Kundendaten unterliegen den Schweizer Datenschutzbestimmungen und der EU Datenschutz Direktive.
- Alle Kundendaten werden mittels AES-256 verschlüsselt auf der Festplatte gespeichert.
- Passwörter werden als SHA-256 Hash und einem individuellem Salt gespeichert.
- Alle Kundendaten werden in einem redundant ausgelegten Datenbank Replika Set für hohe Verfügbarkeit gespeichert.
- Die Datenbankinhalte werden zusätzlich mit Off-Site Backups gesichert.
- Alle Verbindungen zwischen Server Instanzen werden mittels SSL verschlüsselt.
- Alle Verbindungen zwischen Clients und unseren Servern werden mittels HTTPS verschlüsselt.
- Wir verwenden nur sichere SSL Chiffren und starke Verschlüsselungsparameter und erhalten eine A+ Bewertung in den Qualy's SSL Labs Tests für unsere Webdienste.
- Wir forcieren verschlüsselte Verbindungen mittels HTTP zu HTTPS Weiterleitung und HTTP Strict Transport Security (HSTS) und sind in den HSTS Preload Listen aller moderner Browser.
- Zwischen den rechtlichen Entitäten sind überall Auftragsdatenverarbeitungs-Vereinbarungen in Kraft.

Authentifizierung und Autorisierung

Für die Authentifizierung und Autorisierung hat **Allthings** folgende Sicherheitsstandards umgesetzt:

- Datenbankzugriff wird mittels feingranulierter Autorisierungs-Scopes limitiert.
- Autorisierung von Clients wir mittels des sicheren Standards OAuth 2.0 implementiert.
- Anfragen an die API werden nur mit einem gültigen, Zeit-limitierten Zugriffs-Token akzeptiert.
- Zugriffs-Token werden nur Nutzern mit einer authentifizierten Sitzung zur Verfügung gestellt.
- Sitzungs-Cookies sind nicht mittels JavaScript zugreifbar (HTTP-only).
- Sitzungs-Cookies sind nur für die individuelle Client Domain gültig.