Allthings

Factsheet # 2

Security Standards

This factsheet provides an overview of the security measures taken by Allthings regarding hosting, data transfer and storage as well as authentication and authorization.

Author	Marco Lüthy
Role	Head of Engineering
Contact data	marco.luethy@allthings.me
Classification	Confidential
Versioning	05.06.2019

Hosting

The following regulations ensure the safety of our **Allthings** hosting environment:

- The web services are running in their own private cloud with a separate public and private network.
- All web services are load balanced with auto-scaling to handle traffic spikes.
- Firewall rules restrict access to the cloud service based on IP and Protocol rules. HTTP and HTTPS are the only accessible protocols to the public internet.
- All resources are monitored in real-time with advanced health checks that monitor not only instance health but also application errors.
- Container instances are automatically restarted on failure.
- Instances are automatically replaced if their health checks fail.
- The hosting data center meets the requirements of an extensive list of global security standards, including ISO 27001, PCI DSS Level 1, IT Grundschutz and the EU Data Protection Directive. Please see AWS cloud compliance for additional information.

Allthings

Data transfer and storage

Regarding data transfer and storage **Allthings** applies the following security mechanisms:

- Customer data is stored in Ireland and never leaves the EU.
- Customer data handling is subject to the Swiss Data Protection Regulations and the EU Data Protection Directive.
- All customer data is encrypted on disk using AES-256.
- Passwords are stored as SHA-256 hash and an individual salt.
- All customer data is stored in a redundant database replica set for high availability.
- The database contents is additionally secured with regular off-site backups.
- All connections between server instances are encrypted via SSL.
- All connections between clients and our servers are encrypted via HTTPS.
- We ensure only secure SSL ciphers and strong encryption parameters are used and receive an A+ rating in the Qualy's SSL Labs test for all our web services.
- We enforce encrypted connections with HTTP to HTTPS redirects and HTTP Strict Transport Security (HSTS) and are in the HSTS preload lists of all modern browsers.
- On a legal level, contract data processing agreements ("Auftragsdatenverarbeitungs-Vereinbarungen") are installed between all legal entities.

Authentication and Authorization

For Authentication and Authorization, **Allthings** has implemented the following security standards:

- Access to database resources is limited by fine-grained authorization scopes.
- Authorization of clients is implemented via the secure standard OAuth 2.0.
- API calls are only accepted with a valid, time-constrained access token.
- Access tokens are only provided to users with an authenticated session.
- Session cookies are not accessible via JavaScript (HTTP-only).
- Session cookies are only valid for each individual client domain.