IT-Sicherheitsprinzipien für Connected Services

Allgemeine Punkte
- SLA-Netzwerkunterstützung und -überwachung rund um die Uhr.
- Separate Umfelder für Fertigungs- und Testvorgänge.
- Servicebereitschafts-Ziel: 99,9%.

Netzwerksicherheit
- Die Server werden in der AWS-Cloud gehostet und durch mehrere Firewalls mit IP-Filterung geschützt.
- Server und Software werden regelmäßig auf Schwachstellen gescannt.
- Die Vorrichtung (Modem plus SIM-Karte) ist ein spezifisches System, das nur zur Datenübertragung an das Netzwerk autorisiert ist und diese spezifische Identität und im Werk geladene Geheimschlüssel benutzt.

Datenschutz
- Databank-Server ist einem Private Cloud-Netzwerk zugeordnet.
- Webportal-Zugriffe sind über HTTPS verschlüsselt und werden alle zwei Jahre erneuert.
- Webserver-Zertifikate werden jährlich erneuert.
- Alle Benutzer-Informationen werden streng nach GDPR verschlüsselt in der Datenbank gespeichert.
- Die Benutzer-Passwort-Speicherung erfolgt über nicht umkehrbare SHA1-Verschlüsselung.

Benutzerzugriff zu Servern und Betriebssystemen
- Passwörter folgen strengen Regeln (Komplexität, Länge, Historie, Sperre usw.).
- Die Benutzer werden nach einer Inaktivitäts-Timeout-Periode automatisch abgemeldet.
- Der gesamte normale und priviligierte Benutzerzugriff zu Software, Systemen, Datenbanken, Netzwerk-Konfigurationen, Funktionen und vertraulichen Daten ist beschränkt und vom Management genehmigt.

Server-Sicherheit
- Die Software-Server sind speziell dediziert.
- Der Serverabsicherungs-Vorgang (unnötige Dienste usw. deaktivieren.) befolgt strenge Regeln.
- Patchingfenster wiederholen sich wöchentlich mit der Möglichkeit der Notbereitstellung von kritischen Out-of-band-Sicherheitspatches für optimale Sicherheit.
- Serversicherheiten folgen streng den Auflagen der Carrier-Organisation und werden durch ein dediziertes Team unterstützt.

Sicherung/Disaster Recovery
- Die monatliche Sicherung wird in allen Umfeldern durchgeführt.
- Es werden tägliche Datensicherungen durchgeführt.

Prüfung
- Regelmäßige IT-Prüfungen und -Auswertungen nach Carrier-Informationssystemen.

Datenzentrum
- Die Connected Services-Infrastruktur wird auf AWS (Amazon Web Service) gehosted und stützt sich auf diese Computer- und Netzsicherheit; um unseren Kunden die optimal gesicherte Cloud zu bieten.

Datenübertragungs-Sicherheit
- Die Geräte-Datenübertragung basiert auf dem LightWeight M2M-Protokoll für dedizierte M2M/IOT-Nutzung.
- Die Datenverschlüsselung basiert auf CoAP (RFC 7252) und DTLS (RFC 6347), mit UDP-Basis.
- Datenübertragungen über öffentliche Netzwerke sind verschlüsselt (z.B. LWM2M…) und verwenden gegenseitige Authentifizierung basierend auf AES-128 Verschlüsselung mit Schlüsselrotation über einen Bootstrap-Mechanismus.