SeeTec
An OnSSI Company

Datenschutz und Datensicherheit in SeeTec Cayuga

Version	Datum
1.1	07.05.2018

Inhalt

Die SeeTec GmbH hat verschiedene Sicherheitsmechanismen / Funktionen in die SeeTec Cayuga Software integriert, um Datenschutz, Datensicherheit und Vertraulichkeit der Daten gemäß der Datenschutzgrundverordnung (DSGVO) sicherzustellen.

1. Verschlüsselte Übertragung zwischen SeeTec Cayuga Server und SeeTec Cayuga Client

- Die Kommunikation zwischen dem Client und den Servermodulen erfolgt verschlüsselt. Hierzu benutzt SeeTec die AES-Verschlüsselung mit einer Key-Länge von 128 Bit
- Das Passwort wird vom SeeTec Cayuga Client an den SeeTec Cayuga Server immer als ,,salted SHA-512 hash" übertagen.
  Zum Schutz vor Man-in-the-Middle-Angriffen werden SSL-Zertifikate eingesetzt.

2. Verschlüsselte Kommunikation zwischen Kamera und SeeTec Server

- Die Übertragung der Audio- und Videoströme von der Kamera zum SeeTec Server kann über HTTPS verschlüsselt werden, sofern die Kamera HTTPS unterstützt.
  Falls von der Kamera unterstützt und von SeeTec für das jeweilige Kameramodell implementiert wird das Protokoll TLS 1.2 verwendet.

3. Bildanzeige / Bildaufzeichnung / Export von Bildmaterial

- Die Bildspeicherung in der SeeTec Cayuga Bilddatenbank (MDB) ist durch ein proprietäres Format geschützt. SeeTec setzt voraus, dass der physikalische Zugang zu dem Aufzeichnungsserver eingeschränkt ist.
- Die Speicherfristen können je Kamera individuell sowie jeweils getrennt für Standard- und Alarmaufzeichnung eingestellt werden.
- Der Bilddatenexport aus der SeeTec MDB heraus ist nach 3DES (Triple DES) verschlüsselt. Der dadurch gegebene Schutz der Rohdaten verhindert eine Manipulation der Rohdaten und stellt damit auch implizit die Authentizität der Daten sicher.
- Zeitbasierte /Ereignisgesteuerte Aufzeichnung ist möglich (z.B.: Aufzeichnung nur außerhalb der Geschäftszeiten und/oder bei einem Ereignis).
- Kameras und Aufzeichnungen können jederzeit ereignisgesteuert aktiviert oder deaktiviert werden.
- Maskierung des Kamerabilds:
  - Sensible Bereiche können durch frei definierbare Formen verdeckt werden.
  - Dynamische Maskierung von bewegten Objekten
  - Beide Methoden stehen sowohl für Liveansicht als auch für Archivbilder zur Verfügung.
  - Alle Maskierungen unterliegen dem Benutzermanagement.

4. Benutzerzugang / Rechteverwaltung

- Pro Benutzer können folgende Rechte individuell vergeben werden:
  - **Überwachungskamera**: Der Benutzer darf eine Kamera und deren Live-Bilder im Überwachungsmodus sehen.
  - **Archiv Kamera**: Der Benutzer darf Kameras im Archivmodus verwenden.
  - **Aufzeichnungen löschen**: Der Benutzer darf Aufzeichnungen im Archivmodus löschen.
  - **Überschreibschutz**: Der Benutzer darf Aufzeichnungen im Archivmodus mit Überschreibschutz versehen bzw. darf einen vorhandenen Überschreibschutz entfernen.
  - Kamer**a-PTZ**: Der Benutzer darf die PTZ-Kamera verwenden, mit Ausnahme von Preset-Kamerapositionen.
  - **Kamerasperre**: Der Benutzer darf die Position der PTZ-Kamera sperren.
  - **Kameraposition verwenden**: Der Benutzer darf die eingestellten Kamerapositionen verwenden.
  - **Kamerapositionen anlegen**: Der Benutzer darf eigene Kamerapositionen anlegen bzw. bereits definierte Positionen löschen.
  - **Kamera exportieren**: Der Benutzer kann im Archivmodus Audio- und Video-Daten im SeeTec-spezifischen Format speichern.
  - **Kamera exportieren (AVI):** Der Benutzer darf im Archivmodus Audio- und Video-Daten als AVI-Datei speichern.
  - **Privacy-Masking**: Der Benutzer darf das Privacy-Masking deaktivieren.
  - **MPEG-Audio**: Der Benutzer darf die Audioübertragung verwenden.
  - **Lageplan**: Der Benutzer darf den entsprechenden Lageplan verwenden.
  - **Ansicht**: Der Benutzer darf festgelegte Ansichten anzeigen lassen.
  - **Button**: Der Benutzer darf Buttons verwenden.
  - **Ereignisauswertung**: Der Benutzer darf die Ereignisauswertung einsehen.
  - **Berichtvorlagen bearbeiten**: Der Benutzer kann im Modus "Ereignisauswertung" Berichtsabfragen erstellen und bearbeiten und sie als Vorlagen speichern.
  - **Servererweiterungen**: Der Benutzer darf Servererweiterungen wie Kennzeichenerkennung verwenden.
  - **Zählungsauswertung**: Der Benutzer kann die Zählungsauswertung im Menü "Ansicht" verwenden.
  - **Kennzeichengruppe verwenden**: Der Benutzer darf Kennzeichengruppen verwenden.
  - **Kennzeichengruppe ändern**: Der Benutzer darf Kennzeichengruppen ändern.
  - **Zutrittskontrolle**: Der Benutzer darf die Zutrittskontrolle verwenden.
  - **Editor für Zutrittskontrolldaten**: Der Benutzer kann den Editor für Zutrittskontrolldaten im Menü "Ansicht" verwenden.

- Für jeden Benutzer kann optional ein zweites Passwort vergeben werden („4 Augen Prinzip“).
- Optional kann der Benutzer gezwungen werden, das Passwort regelmäßig zu ändern.
- Sicheres Passwort: Falls die Option "Benutzer muss ein sicheres Passwort verwenden" aktiviert ist, muss das Passwort mindestens acht Zeichen, darunter mindestens eine Ziffer, einen Groß- und einen Kleinbuchstaben, enthalten.
- Es existiert eine zeitlich begrenzte Anmeldesperre nach drei nicht erfolgreichen Anmeldeversuchen (Schutz vor Brute-Force-Angriffen).
- Abgestufte Rechteverwaltung für Benutzer und Gruppen.
- Abgestufte Rechteverwaltung für Filialadministratoren.
- Keine „Hintertür“ im SeeTec System, um verlorengegangene Administrator-Passwörter wiederherzustellen.
- Zeitbasierter Zugriff auf Live- und Archivbilder möglich (z.B. Zugriff nur außerhalb der Geschäftszeiten).
- Unterstützung von Microsoft Active Directory.

5. Ereignisauswertung / Protokollierung

Folgende Handlungen und Ereignisse werden mit Angabe von Datum und Uhrzeit protokolliert:

- Benutzeranmeldung.
- Modus-Wechsel (Überwachungs-, Archiv-, Ereignis- bzw. Konfigurationsmodus).
- Archivzugriff mit Angabe von Kamera und Zeitpunkt des Archivs.
- Exportvorgänge mit Angabe von Kamera und Zeitpunkt des Exports.
- Kameranutzung mit Angabe der Nutzungsdauer.
- Wächterrundgänge.
- Aktionen (ausgelöst durch Schaltflächen).
- Start der Alarmszenarien sowie Eingaben durch Benutzer, die zur Abarbeitung des Ereignisses erforderlich sind.
- Konfigurationsänderung von Kameraparametern.
- Informationen zu den SeeTec Diensten.
- Speicherung von Audio- und Video-Daten.

Die Handlungen/Ereignisse werden in der SeeTec Verwaltungsdatenbank gespeichert und gemäß den Einstellungen des Errichters/Betreibers nach einem fest definierten Zeitraum gelöscht.
Der Zugriff auf diese Daten erfordert ein spezielles Recht in der SeeTec Benutzerkonfiguration

6. Referenzbildvergleich

Es steht ein automatischer sowie ein manueller Referenzbildvergleich zur Verfügung, mit dem die Einhaltung des einmal vereinbarten Bildausschnittes zyklisch überwacht werden kann.

7. UVV Kassen- und Fiducia-Zertifizierung

Einsatz der SeeTec Cayuga Software im Bankenumfeld ist durch die UVV-Kassen- und Fiducia-Zertifizierung problemlos möglich.

8. DSGVO: Verarbeitung und Übermittlung personenbezogener Daten

Grundsätzlich können Audio- und Videodaten verarbeitet werden, wobei die Audiodaten standardmäßig per Konfiguration deaktiviert sind. In wie weit es sich bei den genannten Daten um personenbezogene Daten gemäß der Datenschutzgrundverordnung (DSGVO) handelt, hängt davon ab, ob eine Identifizierbarkeit in den verarbeiteten Daten möglich ist.
Audio- und Videodaten können über verschiedene Schnittstellen (SDK, SGS; SAI) an Drittsysteme übermittelt werden, bzw. Programmteile der SeeTec Software können in Drittsystemen eingebunden werden, um Audio- und Videodaten anzuzeigen.

9. DSGVO: Speicherung personenbezogener Daten/Protokollierung

- Audio- und Videodaten werden gemäß den Einstellungen des Errichters/Betreibers gespeichert bzw. gelöscht.
- Benutzerdaten (SeeTec Benutzername und Zeitpunkt des Logins) werden im Client-Logfile (`client.log` unter `C:\Users\[Windows Benutzername]\AppData\Local\SeeTec\log`) und im Logfile des Core-Dienstes (`core.log` unter `C:\Program Files\SeeTec\log`) gespeichert.
- Die Logfiles werden gemäß den Einstellungen des Errichters/Betreibers gespeichert bzw. überschrieben.
- Benutzerinteraktionen (Siehe Kapitel 5 Ereignisauswertung/Protokollierung) werden in der Verwaltungsdatenbank gespeichert und gemäß den Einstellungen des Errichters/Betreibers nach einem fest definierten Zeitraum gelöscht. Der Zugriff auf diese Daten erfordert ein spezielles Recht in der SeeTec Benutzerkonfiguration.
- Benutzerdaten (SeeTec Benutzername und Passwort) können im Client-Login-Dialog gespeichert werden. Die Benutzerdaten werden verschlüsselt in der Datei `client.conf.xml` abgelegt (Speicherort: `C:\Users\[Windows Benutzername]\AppData\Local\SeeTec\`).
- Für den E-Mailversand von z.B. Systemnachrichten oder Alarmbenachrichtigungen werden gegebenenfalls personenbezogene E-Mailadressen durch einen SeeTec Administrator im Konfigurationsmodus unter System-> E-Mail-Verwaltung eingetragen und gespeichert.

10. SeeTec Software Development Kit (SDK)

Anwendungen, die das SDK integrieren, verhalten sich bezüglich Datensicherheit und Datenschutz wie ein SeeTec Cayuga Client. (Siehe auch Kapitel 1 Verschlüsselte Übertragung zwischen SeeTec Server und SeeTec Client).
Es werden die gleichen Daten abgerufen und gespeichert, zur Anmeldung ist ein gültiger Benutzeraccount nötig. Zur Datennutzung außerhalb des SDKs muss der Hersteller der jeweiligen Anwendung befragt werden.

11. SeeTec Gateway Service (SGS), SeeTec Transcoding Service (STS)

Anwendungen, die das SGS nutzen, verhalten sich bezüglich Datensicherheit und Datenschutz wie ein SeeTec Cayuga Client.
Es werden die gleichen Daten abgerufen und gespeichert, zur Anmeldung ist ein gültiger Benutzeraccount nötig.
Zur Datennutzung außerhalb des SGS muss der Hersteller der jeweiligen Anwendung befragt werden.
Die Datenübertragung zwischen Anwendung und SGS ist per HTTPS gesichert.
Vom STS transcodierte Videoströme werden über RTSP ausgeliefert und sind nicht verschlüsselt.
Audiodaten werden über das SGS nicht ausgeliefert.

12. SeeTec WebClient, SeeTec MobileClient

SeeTec WebClients und MobileClients verwenden den SeeTec Gateway Service und den SeeTec Transcoding Service. (siehe vorheriges Kapitel SeeTec Gateway Service (SGS), SeeTec Transcoding Service (STS)).

13. SeeTec Access Control Interface (SACI)

Es werden Konfigurationsdaten und Zugangsdaten vom jeweiligen Hersteller-Plug-In abgefragt und in SeeTec Cayuga gespeichert. Die Daten können auch von SeeTec Cayuga Clients abgefragt und angezeigt werden.
Ob dies personenbezogene Daten sind, hängt vom jeweiligen Hersteller-Plug-In ab, ist aber bei einer Zutrittskontrolle sehr wahrscheinlich.
Die Verschlüsselung zwischen dem SACI und dem externen System ist vom externen System abhängig.

14. SeeTec Analytics Interface (SAI)

Videodaten können an das Hersteller-Plug-In übertragen werden; Konfigurations- und Analytics-Daten werden vom jeweiligen Plug-In abgefragt und in SeeTec Cayuga gespeichert, wo sie wiederum auch von SeeTec Cayuga Clients abgefragt und angezeigt werden.
Ob dies personenbezogene Daten sind, hängt vom jeweiligen Hersteller-Plug-In ab, ist aber bei Analytics eher unwahrscheinlich.

15. SeeTec Videoanalyse (VA)

Durch das VA-Modul wird analysiert, ob Videodaten Personen, Fahrzeuge oder sich bewegende Objekte beinhalten, die sich in eine gewisse Richtung oder innerhalb eines definierten Bereichs bewegen. Die Analyseergebnisse (Metadaten) werden zusammen mit den Bilddaten gespeichert.
Die Übertragung der Bilddaten an das Analysemodul sowie die Übertragung der Metadaten an den SeeTec Cayuga Server ist mit TLS 1.2 verschlüsselt.
Für die Konfiguration des VA-Moduls (Regelerstellung) werden Bilddaten an das SeeTec Analytics Server 3D Configuration Tool gesendet. Die Kommunikation ist mit TLS 1.2 verschlüsselt.

16. SeeTec Kennzeichenerkennung (LPR)

Im LPR Modus werden Videodaten analysiert, die Kennzeichen beinhalten. Die Ergebnisse werden in SeeTec Cayuga gespeichert, wo sie wiederum auch von Cayuga Clients abgefragt und angezeigt werden.
Zusätzlich ist es möglich, frei definierbare Stammdaten zu einem Kennzeichen zu hinterlegen, die wiederum personenbezogene Daten zu Halter oder Fahrer enthalten können.
Diese Daten können auch über die SGS Schnittstelle abgefragt werden.

17. Siemens SiPass Integration

Konfigurations- und Zugangsdaten von werden vom Siemens SiPass Server abgefragt und in SeeTec Cayuga gespeichert, wo sie wiederum auch von SeeTec Cayuga Clients abgefragt und angezeigt werden.
Ob dies personenbezogene Daten sind, hängt von der jeweiligen SiPass Installation ab, ist aber bei Zugangskontroll-Software wahrscheinlich.
Zusätzlich ist es möglich, frei definierbare Stammdaten zu einer Zutrittskarte zu hinterlegen, die wiederum personenbezogene Daten enthalten können.

SeeTec GmbH
Werner-von-Siemens-Str. 2–6
76646 Bruchsal, Deutschland
Telefon: +49 7251 9290-0
Telefax: +49 7256 9290-815
E-Mail: info@seetec.de
Internet: https://www.seetec.de