Datensicherheit und Datenschutz

ATOSS Time Control (ATC) besitzt ein umfassendes Berechtigungskonzept um Daten vor Missbrauch oder unberechtigtem Zugriff zu schützen.
Änderungen an Bewegungsdaten (Stempelsätze, Planungen, manuell erstellte Buchungen, Fehlzeiten) bleiben jederzeit nachvollziehbar und werden protokolliert.
Auch bei der Kommunikation bietet ATC ein Höchstmaß an Sicherheit. Der integrierte Webserver kann über kundenseits bereitgestellte Zertifikate auf ssl-Verschlüsselung aufsetzen.

Berechtigungskonzept

ATC bietet ein ausgefeiltes Berechtigungskonzept, das sich flexibel an Anforderungen anpassen lässt. Basis dieses Berechtigungskonzeptes ist eine Authentifizierung des Anwenders gegenüber ATOSS Time Control. Beim Starten der Anwendung wird der Benutzername und das Kennwort abgefragt. Bei der Neuanlage von Benutzern können zufällige Kennwörter vorgegeben und per Email an den Mitarbeiter versendet werden. Des weiteren können Passwortrichtlinien definiert werden, wie z.B. dass Zahlen oder Großbuchstaben im Passwort vorkommen müssen. Zusätzlich besteht die Möglichkeit, die Authentifizierung mit der Anmeldung am Betriebssystem zu verbinden (LDAP-basierte Authentifizierung). Kennwörter werden dadurch nur im Authentifizierungssystem gepflegt. In aktuellen Webbrowsern ist es auch möglich, die bereits mit der Anmeldung am Betriebssystem erlangte Authentifizierung zu nutzen. Die erneute Authentifizierung bei der Nutzung von ATOSS Time Control entfällt dadurch. Die in ATC verfügbaren Berechtigungen unterteilen sich in Navigationsberechtigungen, Ansichtsberechtigungen, Funktions- und Datenberechtigungen sowie Bewegungsdatenrechte (Einschränkungen auf gezielt definierte Mengen von Mitarbeitern und Daten). Grundsätzlich kann bei allen Datenberechtigungen die Art des Zugriffes durch den Anwender auf die Berechtigung lesen – neu – ändern - löschen gesetzt werden. Für die Bewegungsdaten können auch relative Zeiträume vergeben werden, zu denen die Daten im Zugriff stehen.

Durch Stamm- und Bewegungsdatenrechte wird der Zugriff eines Anwenders auf alle Stamm- und Bewegungsdaten, speziell auch mitarbeiterbezogene Daten geregelt.
Diese Einschränkungen können nach organisatorischen Aspekten wie Kostenstellen und Abteilungen oder anhand von Nummernkreisen bzw. Wildcards für Bezeichnungen oder Kürzel (sofern vorhanden) getroffen werden. Der Anwender ist dann ausschließlich dazu berechtigt die Personen und die Daten der gewünschten Bereiche zu bearbeiten.
Daneben existieren noch rollenbasierte Berechtigungen für Abteilungen (ein Verantwortlicher und mehrere Leiter), für Arbeitsplätze (ein Verantwortlicher und mehrere Leiter für die Planung), für Kostenstellen (ein Verantwortlicher und mehrere Leiter), Projektleiter (wer darf Projekte administrieren) und Projektmitarbeiter (wer darf welche Projekte zur Buchung verwenden).
Zudem lassen sich auch Navigations- und Ansichtsberechtigungen einstellen mit denen Zugriffe auf bestimmte Masken erlaubt werden. Auch einzelne Auswertungen und Spaltendefinitionen für Auswertungen und tabellarische Zeitdatenbearbeitung in der Software können über Berechtigungsgruppen vor unbefugtem Zugriff geschützt werden. Fehlzeitengründe können auf Wunsch anonymisiert dargestellt werden. Für jede Berechtigungsgruppe wird definiert, ob den zugehörigen Mitarbeitern die tatsächliche oder die anonyme Darstellung gezeigt wird.

Nachvollziehbarkeit

Die Nachvollziehbarkeit der Änderung von Daten wird im Hinblick auf gesetzliche Vorgaben zur Dokumentationspflicht und Revisionssicherheit von Unternehmen immer wichtiger.
ATC protokolliert Änderungen an Bewegungsdaten automatisch. Der Kunde kann dadurch alle Änderungen und Eingriffe daran jederzeit nachvollziehen.
Die Protokollierung erfasst den jeweiligen Benutzer, den Zeitpunkt des Zugriffes, die Art der Änderung und die konkreten Inhalte, die geändert wurden.
Auch Änderungen an Mitarbeiterstammdaten können versioniert und auch für die Zukunft durchgeführt werden (z.B. Wechsel des Arbeitszeitmodells ab dem 01.01.2019).

Kommunikationssicherheit

Zur Verschlüsselung der Kommunikation zwischen ATC-Client und ATC-Server kann eine VPN-gestützte Datenverbindung als Basis eingesetzt werden.
Die Kommunikation des ATC Geräteprozesses mit den angebundenen Hardwareterminals kann im Bedarfsfall abhörsicher gestaltet werden. Hier bieten die Terminalhersteller unterschiedliche Lösungen an, mit denen sich eine sichere Kommunikation zwischen ATC-Geräteprozess und Terminal realisieren lässt.

ATOSS, Time, Control, Berechtigungskonzept, ssl-Verschlüsselung, Bewegungsdatenrechte, Authentifizierungssystem, Mitarbeiterstammdaten, Hardwareterminal

⇐ Zurück