Sicherheitskonzept samedi® (06/2018)

Ansprechpartner:
Michael Siebert <michael.siebert@samedi.de>, CTO

Schutzbedarf - gespeicherte und verarbeitete Daten

samedi® speichert und verarbeitet personenbezogene und mitunter schützenswerte Daten (nach BDSG § 3). Dabei können diese Daten in folgende Kategorien eingeordnet werden:

1. öffentliche Daten (z.B. Selbstbeschreibung der Praxis, öffentlich buchbare Termine)
2. interne Daten (z.B. Auslastung der Praxis oder einzelner Ressourcen)
3. geheime Daten (z.B. Patientenstammdaten)

Verständlicherweise sind öffentliche und interne Daten weniger sensibel als beispielsweise patientenbezogene Daten. Um diese zu schützen, wurde eigens eine clientseitige Verschlüsselungslösung konzipiert und implementiert. Dieses Verfahren gewährleistet, dass die Daten erst im Client-System von den berechtigen Benutzern entschlüsselt werden können.

Risiken

Gerade bei schützenswerten Daten wie Patientenstamm- oder medizinischen Daten sind die Auswirkungen von Datenverlusten und Angriffen von Außen enorm.
Folgende Risiken bestehen:

a) Unbefugter Datenzugriff
1. Unvorsichtigkeit/ Nachlässigkeit -> dadurch Zugriff durch Unberechtigte
2. Vorsätzliche Weitergabe / Datenmissbrauch durch Berechtigte
3. Durch Angriffe (z.B. DDoS)

b) Nichtverfügbarkeit der Anwendung
1. Durch Hardwarefehler
2. Durch Angriffe (bspw. DDOS)
3. Durch Softwarefehler

c) Datenverlust
1. Durch Hardwarefehler
2. Durch Softwarefehler

Restrisiko

Leider existiert immer ein gewisses Restrisiko, dem nur schwer zu begegnen ist. Darunter fallen beispielsweise die vorsätzliche Weitergabe von Daten durch Berechtigte. Selbst durch sorgfältige Auswahl entsprechend berechtigter Mitarbeiter kann dieser Unsicherheitsfaktor nicht gänzlich ausgeschlossen werden. Auch ein nachlässiger Umgang mit Zugangsdaten kann nicht vollständig verhindert werden.

Maßnahmen

Physischer Hardware-Zugriff

Die Anwendungen der samedi GmbH werden im Rechenzentrum der filoo GmbH in Frankfurt am Main gehostet, welche für den reibungslosen, störungsfreien Betrieb, sowie die physische Sicherheit Sorge trägt. Das Rechenzentrum ist nach dem international anerkannten Standard für Informationssicherheit DIN ISO/IEC 27001 zertifiziert (Zertifikat siehe Datenschutzpaket der samedi GmbH).
Es wird sichergestellt, dass kein unberechtigter Dritter physischen Zugriff auf die Server erhält. Ebenso wird gewährleistet, dass niemand, der physischem Zugriff auf die Serversysteme hat, die Kennwörter und Zugangsdaten zu den Systemen erhält.
Zusätzlich besitzt das Rechenzentrum die Zertifizierung "TIER III" hinsichtlich Qualität, Verfügbarkeit und Sicherheit[1], welche in ganz Deutschland nur von wenigen Hostern erreicht wird.

Schutz gegen Hardware-Fehler

Alle essentiellen Komponenten der Server, also sowohl Hard- als auch Software, sind redundant ausgelegt, um einen Single Point Of Failure zu vermeiden.
Dazu gehören:

- Netzteile
- Festplatten (RAID-1 bei den Anwendungsservern, RAID-5 bei den Datenbankservern)
- Strom- und Netzwerkverkabelung
- Load-Balancer
- Server-Typen (mind. je 2 Anwendungs- und Datenbankserver)

Alle Komponenten sind mindestens mit einer N+1 Redundanz ausgelegt, d.h. dass zu jeder Systemkomponente mindestens eine Ersatzkomponente bereitsteht, die bei eventuellen Ausfällen einspringen kann.

[1] https://www.filoo.de/rechenzentrum.html

Zugriff auf die Systeme

Zugriff auf die Anwendungs- und Datenbankserver haben nur einzelne, durch die samedi® GmbH bestimmte und entsprechend qualifizierte Mitarbeiter der samedi GmbH. Alle Mitarbeiter sind zur Geheimhaltung verpflichtet.
Die Systeme sind durch Firewalls und entsprechend gehärtete Konfigurationen aller Systemkomponenten gegen unbefugten Zugriff von außen abgesichert. Regelmäßige Updates der Software-Komponenten werden durch die Administratoren durchgeführt, überwacht und automatisiert auf die Server verteilt.

Als zusätzliche Maßnahme zum Schutz vor unbefugtem Datenzugriff sind auch die Festplatten der Datenbankserver AES-verschlüsselt, mit einer Schlüssellänge von 256 Bit. Dadurch können die DB-Server ohne Kenntnis des Festplattenkennworts nicht einmal hochgefahren werden. Das Kennwort selbst ist nur den Administratoren der Server bekannt.

Zugriff auf Anwendungsebene

a) Übertragung der Daten
Der Zugriff auf die samedi®-Anwendung durch die Benutzer ist nur über eine SSL-verschlüsselte HTTP-Verbindung möglich.
Die eingesetzten Algorithmen werden jeweils nach dem aktuellen Stand der Technik sowie nach den technischen Richtlinien des BSI ausgewählt (vgl. TR-03116-4 und TR-02102). Ebenfalls wird regelmäßig ein SSL Testing Tool wie z.B. von Qualys ausgeführt (, Note A+)

Stand Dezember 2015 werden folgende Cipher-Suites unterstützt:

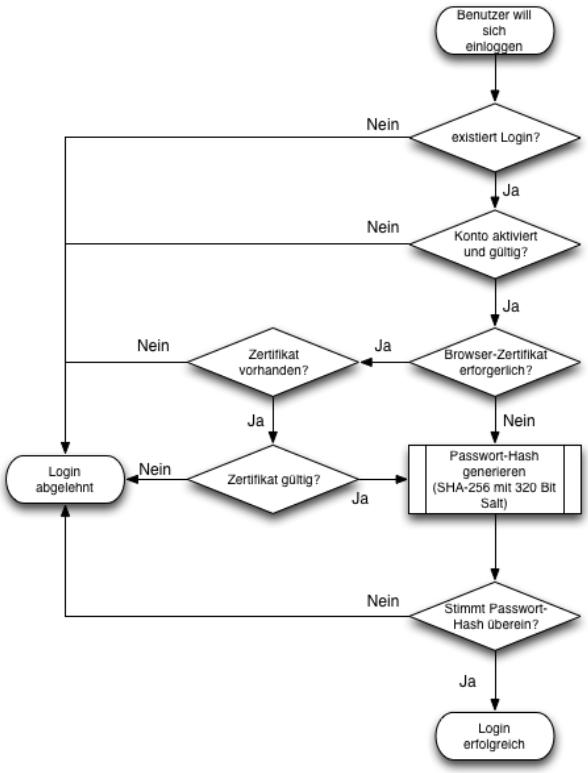
ECDHE-RSA-AES256-SHA
DHE-RSA-AES256-SHA
DHE-RSA-CAMELLIA256-SHA
AES256-SHA
CAMELLIA256-SHA
DES-CBC3-SHA
ECDHE-RSA-AES128-SHA
DHE-RSA-AES128-SHA
DHE-RSA-CAMELLIA128-SHA
AES128-SHA
CAMELLIA128-SHA
ECDHE-RSA-AES256-SHA
DHE-RSA-AES256-SHA
DHE-RSA-CAMELLIA256-SHA
AES256-SHA

CAMELLIA256-SHA
DES-CBC3-SHA
ECDHE-RSA-AES128-SHA
DHE-RSA-AES128-SHA
DHE-RSA-CAMELLIA128-SHA
AES128-SHA
CAMELLIA128-SHA
ECDHE-RSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-SHA384
ECDHE-RSA-AES256-SHA
DHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-SHA256
DHE-RSA-AES256-SHA
DHE-RSA-CAMELLIA256-SHA
AES256-GCM-SHA384
AES256-SHA256
AES256-SHA
CAMELLIA256-SHA
DES-CBC3-SHA
ECDHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-SHA256
ECDHE-RSA-AES128-SHA
DHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA
DHE-RSA-CAMELLIA128-SHA
AES128-GCM-SHA256
AES128-SHA256
AES128-SHA
CAMELLIA128-SHA

Als unsicher geltende Konfigurationen werden bei Bekanntwerden gesperrt. Ebenfalls nutzen wir non-Standard 2048 Bit DH-Parameter.

b) Zugriff/Authentifizierung zum System

Zur Authentifizierung benötigt der Benutzer einen Benutzernamen und ein Passwort. Richtlinien über die Komplexität der Passwörter werden - soweit technisch möglich - überprüft (z.B. werden zu kurze Kennwörter abgelehnt).
Die Passwörter werden in der Datenbank nach dem aktuellen Stand der Technik als SHA256-Hash mit 320bit Salt gespeichert.
Zusätzlich besteht die Möglichkeit für die Benutzer ein Browser-Zertifikat anzulegen, durch das der Zugriff mit Benutzername und Passwort nur von den PCs mit den entsprechenden Zertifikaten erfolgen kann. Dieses Zertifikat sorgt damit für eine Authentifizierung des Rechners und beschränkt den Zugriff auf bspw. die Rechner der ärztlichen Behandlungseinrichtung.
Diese Zertifikate werden mit eine Schlüssellänge von 2048 Bit generiert und sind 3 Jahre gültig. Da sie nur zur Authentifizierung des Rechners und NICHT des Benutzers genutzt werden, sind diese von einer privaten, durch uns erstelleten CA generiert.



c) Zugriff auf die Daten

Jede Praxis hat lediglich Zugriff auf ihre eigenen Daten und kann anderen Praxen über ein Rechtevergabesystem die Rechte vergeben, Termine in den eigenen Kalender einzutragen (sog. Zuweiserfunktion) und Informationen (z.B. Nachrichten) darüber austauschen.
Patientendaten können allerdings in keinem Fall von Dritten eingesehen werden - auch nicht von Mitarbeitern oder Administratoren der samedi® GmbH. Dazu wurde eigens ein auf asymmetrischer Kryptographie basierendes Verschlüsselungssytem entwickelt, implementiert und zum Patent angemeldet[2]. Dabei haben alle symmetrischen Schlüssel eine Länge von 256 Bit, alle asymmetrischen Schlüsselpaare haben eine Länge von 2048 Bit. Details über das Verschlüsselungssytem können der Patentschrift entnommen werden.

d) Sicherheits- und Zugriffskonzept

Das samedi® Sicherheits- und Zugriffskonzept sieht vor über die Kontoeinstellungen Beschränkungen für die Institution sowie für Benutzer festzulegen und die Logins zu kontrollieren.

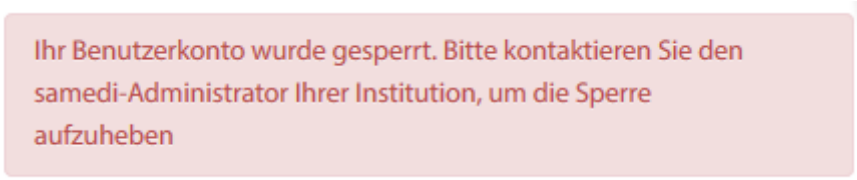
1. Benutzersperrung nach mehrfach fehlerhafte Loginversuchen
2. Automatisches Logout nach inaktiver Zeit
3. Manuelles Auslösen einer Passwort-Änderung durch Administrator
4. Kontrolle des Zugriffs einzelner Benutzer auf samedi durch Einschränkung von IP Adressen
5. Einstellung von Benutzergruppen zur Funktionsbeschränkung von Benutzern
6. Blockierung oder Löschung nicht benötigter Benutzer

[2] Veröffentlichungsnummer: EP000002110980A2; einzusehen unter http://bit.ly/pHwkCf

Sicherheitskonzept samedi® (Stand 06/2018)
samedi GmbH, Rigaer Straße 44, 10247 Berlin

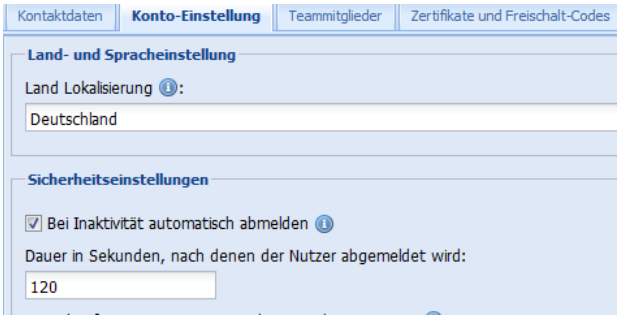
1. Benutzersperrung nach mehrfach fehlerhaften Loginversuchen

Der Zugang zum samedi Account wird automatisch gesperrt, sobald der User 10x ein falsches Passwort beim Login angibt. Diesem User ist der Zugriff für 1h verwehrt. Ein Admin-Nutzer kann die Sperrung für den User wieder aufheben. Für den Benutzer erscheint folgender Hinweis:



2. Automatisches Logout nach inaktiver Zeit

Jeder User kann in den Einstellungen eine weitere Sicherheitseinstellung vornehmen. Über die "Konto Einstellung" unter dem Reiter "Institution" lässt sich die autom. Abmeldung bei Inaktivität für die Institution festlegen. Die Abmeldung bei einer Inaktivität kann pro Institution eingestellt werden.



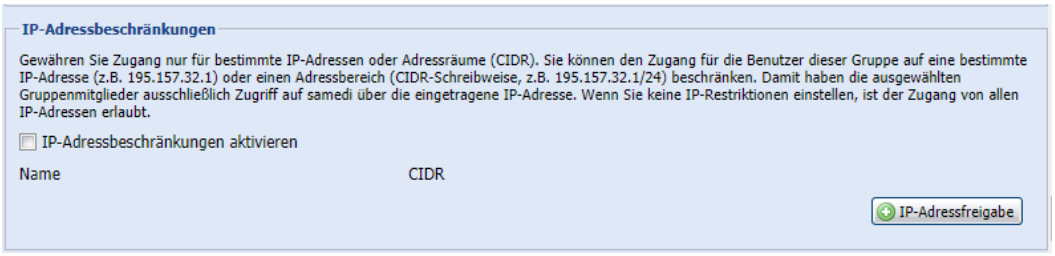
3. Manuelles Auslösen einer Passwort-Änderung durch Administrator

Einem samedi Nutzer mit Administrator-Rechten ist es möglich für einzelne Benutzer beim nächsten Login eine Passwort-Änderung anzufordern. Das Auslösen der Passwort-Änderung kann jederzeit manuell durch den Administrator eingestellt werden. Über die "Institution" und dann direkt in dem Benutzer kann die Einstellung angefordert werden.

Für den ausgewählten Benutzer
erscheint beim nächsten Login der Hinweis,
dass ein neues Passwort gewählt werden muss.

4. Kontrolle des Zugriffs einzelner Benutzer auf samedi durch Einschränkung von IP Adressen

Über die Einstellung der Benutzergruppen ist es möglich den Zugang zu samedi nur für bestimmte IP-Adressen oder Adressräume (CIDR) zu gewähren. Der Zugang für die Benutzer lässt sich auf eine bestimmte IP-Adresse (z.B. 195.157.32.1) oder einen Adressbereich (CIDR-Schreibweise, z.B. 195.157.32.1/24) beschränken. Damit kann gesichert und kontrolliert werden, von welcher IP Adresse sich die Benutzer einloggen. Loggt sich ein Benutzer dann von einer anderen IP Adresse ein, erscheint eine Fehlermeldung. Wenn keine IP-Restriktionen eingestellt werden, ist der Zugang von allen IP-Adressen erlaubt.
Die IP-Adressbeschränkungen lassen sich unter "Einstellungen", dem Bereich "Institution" und dann unter dem Reiter "Benutzergruppen" einstellen. Ganz unten in der Verwaltung der Benutzergruppe finden Sie die IP-Adressbeschränkungen. Es lassen sich auch mehrere IP-Adressen angeben.



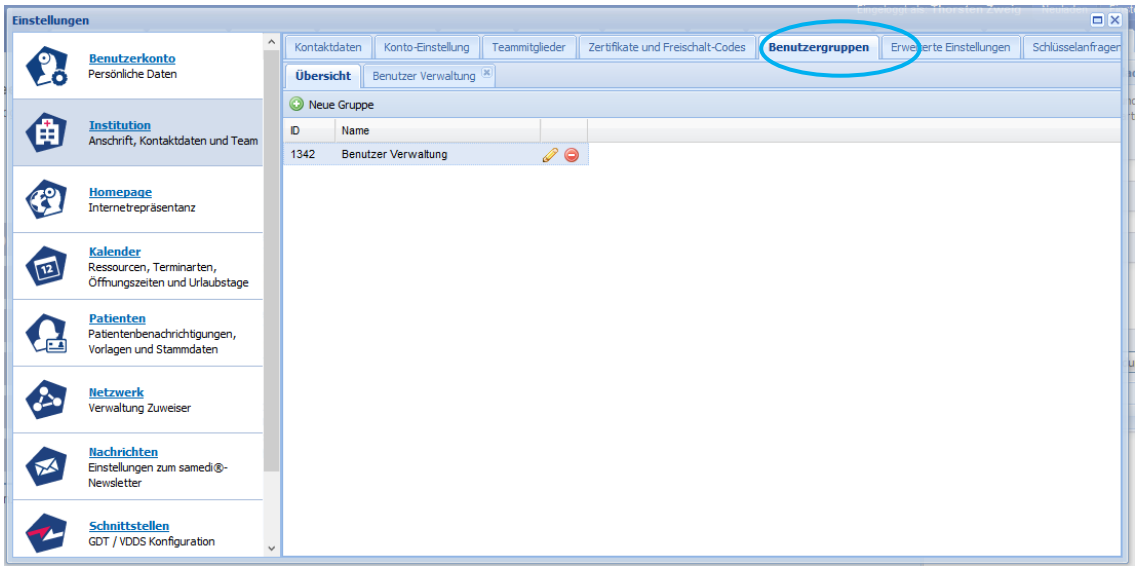
5. Einstellung von Benutzergruppen zur Funktionsbeschränkung von Benutzern

Das Rollenkonzept sieht es vor Benutzerkonten zu unterteilen in:

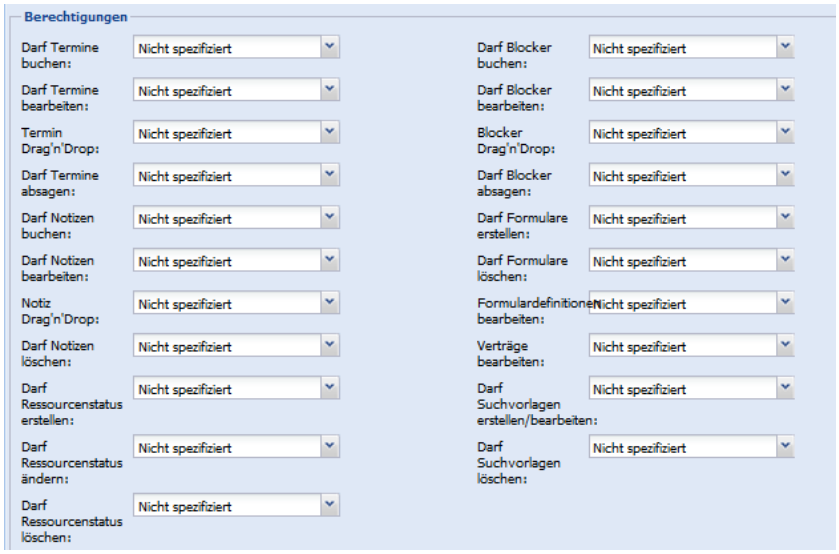
- Normaler User (verfügt über die Standardzugriffsmöglichkeiten)
- Administrator (erhält Zugriff auf Einstellungen und kann Konfigurationsänderungen vornehmen)
- Master-User (nur im Falle eines Passwort-Verlustes aller Mitglieder und zur Rettung des Institutionskontos, sodass Zugriff auf das samedi® Konto weiterhin möglich ist)

Funktionale Einzelheiten:

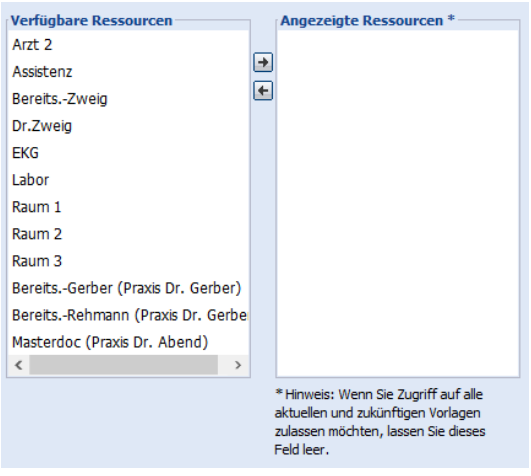
Als samedi® Administrator können für die einzelnen User/Teammitglieder innerhalb der samedi®-Lösung spezielle Berechtigungen gesetzt oder entzogen werden. Über die Funktion "Benutzergruppen" können die Berechtigungen pro User definiert und jederzeit verändert werden. Das dafür vorgesehene Einstellungsmenü finden Sie unter >> Einstellungen >> Institution >> Benutzergruppen, wie die nachfolgende Abbildung zeigt.



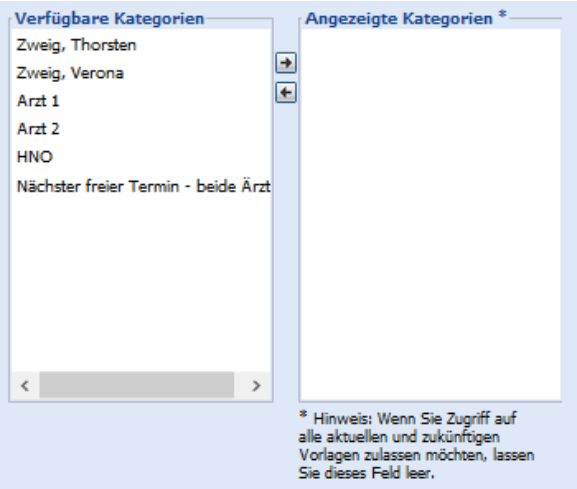
Dabei richtet sich der genaue Funktionsumfang anhand der gebuchten Module/Pakete. Der User hat folgende Berechtigungen zu darf / darf nicht:



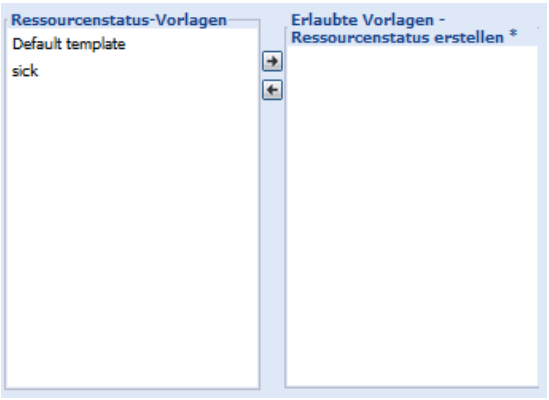
a) Welche **Ressourcen** der Benutzergruppe angezeigt werden.



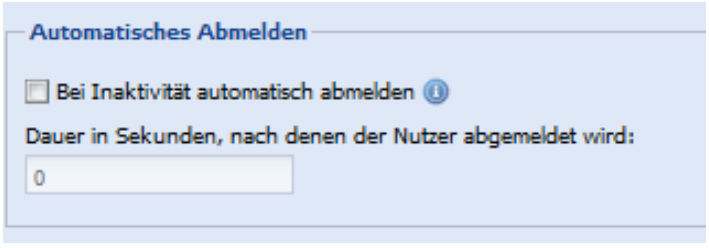
b) Welche **Kategorien** der Benutzergruppe angezeigt werden.



c) Wer erlaubte **Ressourcenstatus-Vorlagen** erstellen, bearbeiten und löschen darf.

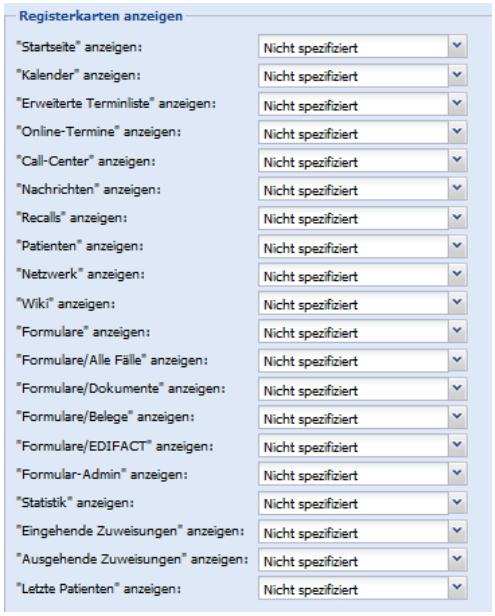


Außerdem kann aus Sicherheitsgründen ein automatisches Log-Off für die Benutzer innerhalb der Benutzergruppe angewendet werden. Sie bestimmen hierbei die Zeit bei welcher der Benutzer im Falle der Inaktivität aus samedi® abgemeldet wird.



Des Weiteren können für das samedi®-Konto bestimmte **Registerkarten** ausgeblendet werden. In Abhängigkeit der verfügbaren Module können Benutzer voll oder gar nicht auf folgende Reiter zugreifen:

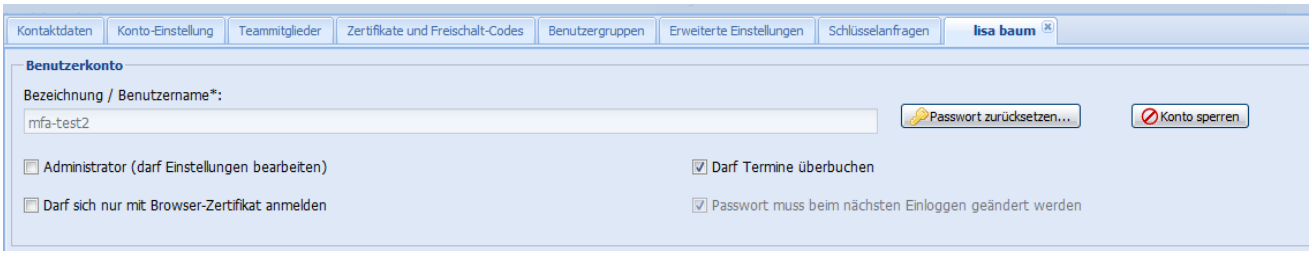
- Startseite
- Kalender
- Erweiterte Terminliste
- Online-Termine
- Call-Center
- Nachrichten
- Recalls
- Patienten
- Netzwerk
- Wiki
- Formulare
- Formulare/Alle Fälle
- Formulare/Dokumente
- Formulare/Belege
- Formulare/EDIFACT
- Formular-Admin
- Statistik
- Eingehende Zuweisungen
- Ausgehende Zuweisungen
- Letzte Patienten



6. Blockierung oder Löschung nicht benötigter Benutzer

Nicht mehr benötigte Benutzer einer Institution können von einem Administrator in samedi entweder blockiert oder gelöscht werden. Damit ist der Zugriff auf samedi von nicht mehr authorisierten Personen nicht mehr möglich.
Benutzer können gelöscht werden über: "Einstellungen" und dann "Teammitglieder"

Benutzer können deaktiviert werden über: "Einstellungen", dann "Institution" und dann "Teammitglieder". Über einen Doppelklick auf den Benutzer lässt sich dieser Zugang dann sperren.



Die Sperrerung kann jederzeit wieder von einem Administrator aufgehoben werden.

Datenschutzbeauftragter

Datenschutzbeauftragter der samedi® GmbH ist Herr Dr. Tobias Wauschkuhn, der nach der EU-Datenschutz-Grundverordnung (gem. Art. 37 EU-DSGVO) folgende Aufgaben übernimmt:

- Hinwirken auf Einhaltung der Datenschutzbestimmungen
- Überwachung der Datenverarbeitung
- Durchführen von Vorabkontrollen
- Vertrautmachen der Mitarbeiter mit geltenden Vorschriften und besonderen Erfordernissen
- Ansprechpartner für Geschäftsleitung, Mitarbeiter, Kunden, Dritte

Backups

Um einem Datenverlust im Fehlerfall zu vermeiden, wurde ein mehrstufiges Backup-System implementiert. Alle schützenswerten Daten werden in einer PostgreSQL Datenbank gespeichert. Um einem Datenverlust vorzubeugen, müssen daher lediglich die Verfügbarkeit, Integrität und Vertraulichkeit der Daten in dieser Datenbank gewährleistet werden. (Selbstverständlich treffen diese Schutzziele auch bei anderen Komponenten wie bspw. Anwendungsservern zu, sind aber in der Betrachtung der Backups außer Acht zu lassen).

Stufe 1: Replikation auf Hot-Standby

Häufigkeit: Kontinuierlich
Vorhaltezeit: nicht zutreffend

Die erste Stufe stellt eine Replikation der PostgreSQL Datenbank auf einen sog. Hot-Standby-Server dar. Da dies mittels der von PostgreSQL bereitgestellten "Streaming Replication" funktioniert, ist hier nahezu eine Echtzeit-Replikation im Gange. Durchschnittlich dauert es weniger als 10ms, bis Änderungen vom Master-Server auf das Replica gespiegelt werden. Dieses Master-Slave-Replikation kann genutzt werden, wenn der Primäre Datenbank-Server ausfällt oder gewartet werden muss. Ein Umschalten zwischen den Servern dauert im Fehlerfall wenige Sekunden.

Stufe 2: Datenbank-Backup im eigenen Rechenzentrum

Häufigkeit: Kontinuierlich
Vorhaltezeit: 2 Wochen

Die zweite Stufe ist eine kontinuierliche Replikation der Datenbank auf einen dritten Backup-Server

mittels PGBarman und PostgreSQL-Hausmitteln wie WAL-Archiving und Streaming Replication. Hierdurch sind alle Daten der Datenbank ein weiteres Mal im Rechenzentrum vorhanden. Sollten also sämtliche Festplatten in beiden Datenbankservern gleichzeitig Defekte erleiden, kann binnen maximal einer Stunde ein komplett neuer Datenbankserver mit aktuellem Datenbestand gestartet werden.

Stufe 3: Datenbank-Backup in Dritt-Rechenzentrum

Häufigkeit: Kontinuierlich
Vorhaltezeit: 60 Tage

Die dritte Stufe ist ein Speichern der Datenbank-Backups an einem anderen Standort. Dazu werden alle Backup-Dateien, nachdem sie von PGBarman verarbeitet wurden, mit GPG asymmetrisch verschlüsselt und in einen S3 Bucket hochgeladen. Damit liegen die Backups verschlüsselt in Amazon AWS-Rechenzentren und haben eine Verfügbarkeit von 99,999999999% auf die gespeicherten Dateien bzw. 99,99% auf die Verfügbarkeit im Zugriff.
Durch die lokale, asymmetrische GPG-Verschlüsselung haben auch nur Administratoren der samedi GmbH Zugriff auf die Backup-Daten. Die S3-Buckets werden ausschließlich im AWS-Rechenzentrum EU (Frankfurt) gespeichert. Für mehr Informationen bzgl der Datensicherheit und Compliance der AWS-Rechenzentren sei an https://aws.amazon.com/de/compliance/ verwiesen.

Löschfristen der Backups

Die Backups werden entsprechend ihrer Vorhaltezeit vorgehalten und am Ende ihrer Lebenszeit automatisiert gelöscht.

Schulung der Mitarbeiter und Anwender

Die Sicherheit wird durch Schulungen von Mitarbeitern und Anwendern gefördert. Dabei werden grundsätzliche Maßnahmen vermittelt, um ein Bewusstsein für den Umgang mit sensiblen Daten zu fördern.
Zu den vermittelten Maßnahmen gehören unter anderem:

- das Verwenden sicherer Passwörter (Mindestlänge, Verwendung einer Kombination aus Ziffern, Buchstaben und Sonderzeichen)
- das regelmäßige Ändern der Passwörter (voreingestellte Passwort nach Erhalt sofort ändern)
- das Ändern von Passwörtern bei Verdacht auf Missbrauch oder unberechtigte Weitergabe von Login-Daten
- der Umgang mit schriftlichen Aufzeichnungen zu Login-Daten

Richtlinien über die Komplexität der Passwörter werden - soweit technisch möglich - überprüft (z.B.

werden zu kurze Kennwörter abgelehnt). Der Umgang mit Passwörtern erfolgt gemäß BSI-Empfehlung und wird in unseren technischen und organisatorischen Maßnahmen genauer beschrieben.

Eine Verpflichtung der samedi-Mitarbeiter zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes erfolgt bezugnehmend auf Art. 28 Abs. 3 S. 2 lit. b DSGVO, §88 TKG und §17 UWG, mit Belehrung über strafrechtliche Konsequenzen im Sinne von Art. 84 DSGVO, §42 DSAnpUG-EU (BDSG-neu) und §206 StGB.

Kosten-Nutzen-Verhältnis

In Anbetracht der besonderen Sensibilität der verarbeiteten medizinischen Daten und des entstehenden Schadens im Falle eines Angriffs oder Missbrauchs, sind die Kosten für die Datensicherheit und den Datenschutz in jedem Fall angemessen.
Daher liegt die Priorität bei allen Aspekten von Konzeption, Entwicklung und Betrieb von samedi® auf der Gewährleistung von Datenschutz und -sicherheit.