

Sicherheitsstatement ilabClient

1. Einleitung

Unsere Softwarelösungen gehen ständig mit hochbrisanten Daten um, die in der Datenschutz-Grundverordnung (DSGVO) „besondere Arten personenbezogener Daten“ genannt werden.

Wir stehen daher vor der Herausforderung, ein hohes Maß an Datensicherheit zu erreichen, ohne die Benutzungsfreundlichkeit unserer Software unangemessen zu beeinträchtigen.

Wir wollen Ihnen mit dem ilabClient eine Lösung an die Hand geben, mit der Sie alle Anforderungen der DSGVO erfolgreich umsetzen können.

Das geht nur durch den gezielten Einsatz der richtigen Mittel im jeweiligen Kontext.

Wie wir dies erreichen, wollen wir hier beschreiben, ohne sicherheitsrelevante Details zu verraten.

2. Zugangssicherheit ilabServer

2.1. Login und Passwort

Die Basis-Authentifizierung am ilabServer, mit der sich der ilabClient gegenüber dem ilabServer authentifiziert, findet über Login und Passwort statt. Richtig angewendet bietet dies bereits einen guten Schutz vor Fremdzugriff. Nach erfolgreicher Authentifizierung erhält der ilabClient Zugang zum ilabServer-System mit den im Vorfeld durch einen Administrator vergebenen Berechtigungen. Bei der Vergabe von Login und Passwort sollte Wert auf eine hohe Komplexität gelegt werden. Eine Mehrfachnutzung dieser Anmeldedaten auch an anderer Software oder Diensten sollte nicht erfolgen.

Allerdings ist es schwer, sich verschiedene komplexe Kennwörter zu merken. Für die Verwaltung empfiehlt sich der Einsatz einer Passwortverwaltungssoftware wie z. B. Keeper, mit deren Hilfe ein Nutzer Kennwörter und Geheimzahlen verschlüsselt speichern, verwalten und in der Regel auch sichere Kennwörter erzeugen kann. Dann muss man sich nur noch ein einziges besonders gutes Passwort merken, das den Zugriff auf die Passwortverwaltungssoftware erlaubt.

2.2. Kennwortkomplexität

In den meisten bekannt gewordenen Fällen von Datendiebstahl ist der Zugang durch nicht autorisierte Personen auf die Vergabe von zu schwachen oder zu häufig verwendeten Kennwörtern zurückzuführen. Kennwörter, die anhand von Wörterbüchern durchprobiert werden können oder z. B. nur aus bis zu 8 Ziffern oder Kleinbuchstaben bestehen, können durch eine Brute-Force-Attacke (systematisches Durchprobieren) mit heutiger starker Hardware innerhalb von Sekundenbruchteilen geknackt werden. Aus diesem Grund sollten in medizinischen Anwendungen möglichst komplexe

Beispiel für ein gutes Passwort:

Man nimmt sich einen Merksatz und bildet daraus die Anfangsbuchstaben, wobei man Ziffern und Satzzeichen integriert.

Merksatz Beispiel:

Ich habe ein schönes Haus, ein großes Auto und zwei tolle Kinder.

Daraus gebildetes Passwort:

Ih1sH,1gAu2tK.

Beispiele für schlechte Passwörter:

87654321

Mehlwurm

Kennwörter gewählt werden. Dafür ist sowohl die Passwortlänge als auch die Zeichenauswahl relevant.

Ein Kennwortgenerator ist ein praxisbewährtes Hilfsmittel zur Erzeugung hinreichend komplexer Passwörter und bereits in unserem ilabServer integriert. Durch diesen Kennwortgenerator wird durch den Support initial ein sicheres Passwort erstellt. Diese 10 oder mehr Zeichen langen Kennwörter sind zufallsgeneriert und enthalten eine beliebige Auswahl von Ziffern, Groß- und Kleinbuchstaben sowie Sonderzeichen. Der Anwender kann, wenn er möchte, dieses initial erstellte Passwort im ilabClient ändern. Hier sollte aber auch darauf geachtet werden, ein nach aktuellem Standard sicheres Passwort zu verwenden. Im ilabServer werden aktivierte Kennwörter nicht im Klartext angezeigt.

2.3. Speicherung der Kennwörter

Die im ilabServer abgelegten Kennwörter werden grundsätzlich als Hash-Wert gespeichert. Mit einem sicheren Zufallszahlengenerator werden Zufallsbytes erzeugt, die dem Hash-Wert als Salt hinzugegeben werden. Es wird auch gespeichert, welche Hash-Funktion verwendet wurde, falls irgendwann modernere Verfahren entwickelt werden, die dann wieder in die Lage versetzt werden müssen, mit den bisherigen Kennwörtern umzugehen.

Selbst wenn zwei gleiche Kennwörter im ilabServer verwendet werden sollten, haben sie nicht den gleichen gespeicherten Hashwert wegen der Zugabe des Salt. So haben Angriffe auf Basis von Hashwert-Tabellen keinen Erfolg.

Wenn Kennwörter für die Anmeldung am ilabServer eingegeben werden oder unsere Software-Komponenten sich automatisch mit Hilfe von Login und Passwort in ein ilabServer-Postfach einwählen wollen, dann werden nur die „gesalzenen“ Hash-Werte miteinander verglichen.

Als zusätzliche Komfortfunktion bietet der ilabClient die Möglichkeit, das Passwort so zu speichern, dass keine erneute Eingabe beim Abruf von Labordaten vom ilabServer benötigt wird. Dies geschieht automatisch, wenn das Passwort für den ilabServer in der Abrufkonfiguration hinterlegt wird. Sollte dies nicht gewünscht sein, so kann das entsprechende Feld einfach leer gelassen werden. Dann muss bei jedem Abruf das Passwort neu eingegeben werden. Wenn das Passwort hinterlegt ist, sollte aber besonderer Wert auf den Schutz des PCs gelegt werden, auf dem der ilabClient installiert ist (vgl. [4.2. Sicherheitsmaßnahmen und lokale Verschlüsselung](#)).

3. Kommunikation mit dem ilabServer

3.1. Sicherheitsfaktoren

Der ilabClient verwendet bei jedem Abruf von Labordaten zum einen die Basis-Authentifizierung sowie eine zusätzliche Verschlüsselung. Als Verschlüsselungsverfahren stehen hierbei die Kryptographie-Software **XKM** oder das **Elliptic Curve Integrated Encryption Scheme (ECIES)** Verfahren zur Verfügung. Welche Verschlüsselung benutzt wird, entscheidet das entsprechende Labor. Beide Verfahren nutzen eine hybride Verschlüsselung, jedoch verwendet ECIES für die Schlüsselgenerierung das **Elliptic-curve Diffie-Hellman (ECDH)** Verfahren, welches deutliche Performance Verbesserung gegenüber dem vom XKM-Modul benutztem **RSA**-Verfahren bietet.

3.2. Hybride Verschlüsselung

Bei der hybriden Verschlüsselung wird zunächst ein asymmetrisches Schlüsselpaar bestehend aus einem privaten und einem öffentlichen Schlüssel im ilabClient generiert. Der private Schlüssel bleibt hierbei jederzeit nur im ilabClient und wird an keinem anderen Ort gespeichert. Der öffentliche Schlüssel wird, geschützt durch eine HTTPS-Verbindung, an den ilabServer übertragen, wo dieser gespeichert wird. Der ilabServer verschlüsselt nun die zu übertragenden Labordaten mithilfe eines einmalig verwendeten symmetrischen Schlüssels. Dieser symmetrische Schlüssel wird im Anschluss mithilfe des öffentlichen Schlüssels des ilabClient verschlüsselt. Diese verschlüsselten Labordaten und der verschlüsselte symmetrische Schlüssel werden dann erneut über eine HTTPS-Verbindung zum ilabClient übertragen. Der ilabClient kann anschließend mithilfe des privaten Schlüssels den symmetrischen Schlüssel und damit wiederum die

Labordaten entschlüsseln. Dies geschieht automatisch durch den ilabClient beim Empfang der Daten.

3.3. HTTPS-Verbindung

Zusätzlich zu den vorher genannten Verschlüsselungen der Labordaten, ist die Verbindung zwischen ilabServer und ilabClient als HTTPS-Verbindung aufgebaut, damit ein sicherer, verschlüsselter Internettransport stattfinden kann (Transport Layer Security Protokoll - TLS). Die jeweilige TLS-Version wird hierbei durch den ilabClient festgelegt. Wir empfehlen mindestens TLS >= 1.2, wenn möglich aber TLS 1.3, zu verwenden, um die maximale Sicherheit der Labordaten zu gewährleisten.

4. Ablage der Labordaten auf dem Ziel-PC

4.1. Speicherung und Zugriff

Nachdem die Labordaten durch den ilabClient verschlüsselt vom ilabServer abgerufen und entschlüsselt wurden, werden sie unverschlüsselt im konfigurierten Zielpfad abgelegt. Dies ist notwendig, damit die abgerufenen Daten problemlos in bestehende Praxissysteme importiert werden können. Die Möglichkeit, die Labordaten direkt in der jeweiligen Praxissoftware weiterzuverarbeiten, stellt den Hauptanwendungsfall des ilabClients dar. Für alternative Nutzungsszenarien, beispielsweise wenn kein direkter Import in eine bestehende Infrastruktur erforderlich ist, bieten wir ergänzende Lösungen an, wie eine browserbasierte Plattform zur Ansicht der Labordaten.

Da der ilabClient die Anmeldedaten für den ilabServer standardmäßig speichert, sollte darauf geachtet werden, dass er in einer gesicherten Umgebung installiert wird. Eine zusätzliche Passwortabfrage für den Start des ilabClients existiert bei der Standardinstallation nicht, so dass ein Angreifer, der Zugriff auf den PC hat, im ilabClient an die sensiblen personenbezogenen Daten gelangen könnte. Gerade bei der Nutzung auf potenziell unsicheren Geräten, wie beispielsweise einem Laptop, der auch außerhalb der Praxisumgebung verwendet wird, empfehlen wir daher den Client-Start nur mit Eingabe eines Passworts zu ermöglichen oder den Einsatz unserer alternativen Lösungen wie der browserbasierten Plattform.

4.2. Sicherheitsmaßnahmen und lokale Verschlüsselung

Der PC, auf dem der ilabClient installiert ist, sollte durch geeignete Sicherheitsmaßnahmen vor unbefugtem Zugriff geschützt werden. Dazu zählen unter anderem ein sicheres Systempasswort, eine Festplattenverschlüsselung, die Nutzung aktueller Antivirensoftware sowie die regelmäßige Installation von Sicherheitsupdates.

Zusätzlich ist die Datenbank des ilabClients individuell entsprechend aktuell gültiger Empfehlungen mit dem symmetrischen Verschlüsselungsverfahren AES-256 verschlüsselt. Das für den Start des ilabClients benötigte Passwort kann optional aus einer Umgebungsvariable ausgelesen oder bei jedem Start manuell eingegeben werden.

5. Protokollierung

Im ilabClient werden alle relevanten Nutzeraktionen sowie Systemereignisse protokolliert. Dies umfasst unter anderem den Abruf inklusive der übertragenen Dateien und Fehlermeldungen.

Die Protokollierung ermöglicht eine effiziente Fehleranalyse, indem sie z. B. aufzeigt, ob eine fehlerhafte Benutzerinteraktion oder eine unvollständige Datenübertragung vorliegt.

Darüber hinaus findet auch eine serverseitige Protokollierung relevanter Ereignisse statt.