Software für den gesamten Pflegebereich

WISSENSDATENBANK ZUR GO ON-PFLEGEDOKUMENTATION

HINWEISE ZUR SICHERHEIT DER GO ON-BROWSERLÖSUNG

Hinweise zur Sicherheit der GO ON – Browserlösung

Grundsätzlich gilt:

Wenn ein Kunde die Anwendung selbst in seinem eigenen „Rechenzentrum“ betreiben möchte, ist er selbst für die Sicherheit verantwortlich und hat dafür Sorge zu tragen.

Wenn die Anwendung beim Kunden in einem Intranet (lokalen Netzwerk) betrieben wird, ist sie demzufolge genauso sicher bzw. unsicher wie eine klassische Windows-Anwendung, die beispielsweise mit einem Terminal-Server bereitgestellt wird. Hier gibt es keine Unterschiede.

Bei einer Cloud-Lösung wird die Anwendung nicht mehr selbst betrieben, sondern bei einem anderen Anbieter als Dienst („Software as a Service“, kurz: SaaS) gemietet. Die Anwendung und Daten befinden sich dann nicht mehr im „Rechenzentrum“ des Nutzers/ Kunden, sondern in der „Cloud“, also im Rechenzentrum von GODO Systems oder sonst wo, wobei der Zugriff über das Intenet erfolgt.

GODO Systems oder das Rechenzentrum garantiert die Sicherheit der Cloud-Lösung. Dafür gibt es Zertifikate usw. Bei einer Auslagerung der Technik bei einer traditionellen Lösung, sind das die gleichen Sicherheitsstandards. Es gibt keine Unterschiede.

Mit dem Begriff „Sicherheit“ sind sowohl der gesicherte Zugriff auf Ressourcen als auch der Datenschutz gemeint. Er umfasst in der Cloud im Wesentlichen dasselbe wie im lokalen Rechenzentrum: Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Zurechenbarkeit und Pseudonymität.

Ganz wichtig ist, dass wir in unserer Lösung (das ist bei Weblösung nicht selbstverständlich) die Oberflächen zusätzlich verschlüsselt haben. Das ist eine zusätzliche Sicherheitsstufe, wie wir eingebaut haben. Möglich macht das auch erst die 2. Generation an Webentwicklungsumgebung. Auch hier ist das somit gleich einer traditionellen Lösung.

Einsatz eines SSL/TLS/HTTPS-Protokolls:

Eines der Grundprobleme, nämlich die Absicherung des Zugriffs auf die Anwendungsdaten bei der Datenübertragung zwischen Kunde und Cloud, wird durch den Einsatz des SSL-Protokolls gelöst. Das SSL-Protokoll verschlüsselt die zwischen Browser und Server ausgetauschten Daten und sorgt dafür, dass vertrauliche Informationen vor dem Ausspähen auf dem Übertragungsweg geschützt sind. Das ist absolut sicher, sofern nicht krimminelle Kräfte am Werk sind - dann ist aber auch jede traditionelle Lösung gefährdet.

Authentifizierung und Autorisierung

Die Anwendung und dazugehörige Web-Services sind passwortgeschützt. Durch die Vergabe von Benutzerrechten wird der Zugriff auf die Anwendung und/oder Anwendungsteile überprüft und zugewiesen.

Kryptographie

Darüber hinaus können Passwörter mit Verschlüsselung/ Kryptographie sicher in der Datenbank gespeichert werden.

VPN

Zusätzlich kann man die Datenübertragung durch den Einsatz eines Virtual Private Networks („VPN“) absichern, was ggfs. mehr Sicherheitsgefühl gibt.

Es gibt also keinen Grund zu zweifeln, ob es Sicherheitslücken gibt. Hier gibt es, durchaus auch begründet aus alten Webanwendungen Bedenken, die aber bei den modernen Lösungen (wir verwenden die modernste AJAX-Technologie) unbegründet sind.

Für Fragen stehen wir gerne zur Verfügung (02131 / 29847 - 0).

GODO Systems GmbH