Abfragen und Mutationen via Web-Browser

Versichertendaten im Kontext Web 2.0

Webbasierte Interaktion zwischen Destinatären und Pensionskassen: Was ist technisch möglich und wo sind die regulatorischen Hürden?

IN KÜRZE

Versicherte, Arbeitgeber und Broker stellen unterschiedliche Anforderungen an die Funktionalität eines Online-Schalters. In jedem Fall muss gewährleistet sein, dass alle nur auf die für sie bestimmten Informationen zugreifen können..

Roger Peduzzi
Leiter Marketing und Verkauf, ICR Informatik AG, Rotkreuz

Pensionskassen-Online-Schalter ermöglichen die Interaktion zwischen Vorsorgeeinrichtungen, ihren Versicherten sowie den angeschlossenen Lohnfirmen. Abfragen, Simulationen und Mutationen können so via Web-Browser erfolgen. Durch den Einsatz solcher Web-Anwendungen können Vorsorgeeinrichtungen den Verwaltungsaufwand und somit die Kosten reduzieren, wenn ein Teil der Tätigkeiten, die heute Pensionskassenmitarbeiter wahrnehmen, künftig von den Versicherten und den angeschlossenen Lohnfirmen übernommen werden.

Grosses Potenzial

Im Vergleich mit E-Banking in der Bankenwelt ist die Entwicklung der Online-Schalter in der beruflichen Vorsorge noch nicht soweit fortgeschritten. Aktuell gibt es relativ viele grosse und mittlere Vorsorgeeinrichtungen, die keinen Online-Schalter einsetzen. Dies obwohl die Vorteile auf der Hand liegen. Der Pensionskassen-Online-Schalter...

- bietet Mehrwert für Versicherte, Arbeitgeber und Broker,
- unterstützt eine durchgängige Geschäftsfallabwicklung,
- entlastet die Pensionskassenmitarbeiter,
- verlagert den Aufwand auf Versicherte, Arbeitgeber und Broker,
- steigert die Effizienz,
- reduziert den Verwaltungsaufwand und damit die Kosten,
- ermöglicht kostenlosen, standortunabhängigen Zugriff und
- gewährt permanente Verfügbarkeit (auch ausserhalb von Bürozeiten).

Und bei Vorsorgeeinrichtungen, die ein entsprechendes Produkt einsetzen, gibt es insbesondere in den Bereichen Mutationen und durchgängige Geschäftsfallabwicklung noch viel Potential für Effizienzsteigerungen. Die Hauptgründe für das Zögern sind schnell gefunden. Zum einen müssen die gesetzlichen Auflagen erfüllt sein. Zum anderen sind Vorsorgeeinrichtungen besonders risikoscheu wenn es um Versichertendaten geht. Das ist auch richtig so, denn die Informationssicherheit, sprich der Schutz der Versichertendaten ist zentral.

Hohe regulatorische Sicherheitsanforderungen

Um den Zusammenhang herzustellen, werfen wir zunächst einen Blick auf die verschiedenen Anspruchsgruppen und ihre Bedürfnisse. Versicherte möchten beispielsweise ihr Vorsorgekapital anschauen, Simulationen durchführen und Geschäftsfälle wie WEF-Vorbezüge anstossen. Lohnfirmen hingegen möchten Pensum-, Lohnänderungen, Eintritte und Austritte melden, Beiträge berechnen und das aktuelle Debitorenkonto sehen. Broker wiederum wollen Offerten mit verschiedenen Planvarianten erstellen.

Um den regulatorischen Anforderung und dem Datenschutz zu genügen, muss sichergestellt werden, dass die verschiedenen Anspruchsgruppen nur die für sie bestimmten Daten sehen. Hier spricht man auch vom Need-to-know-Prinzip. Der Versicherte darf nur seine persönlichen Daten, sprich keine Daten von anderen Versicherten sehen. Der Arbeitgeber wiederum darf nur auf die Daten seiner Mitarbeiter sprich Personendaten, Lohn, Beschäftigungsgrad und Beitragsrechnungen zugreifen aber keinesfalls versicherungstechnische Daten seiner Angestellten wie zum Beispiel Spargutthaben, Versicherungsvorbehalt oder Vorbezüge und Einkäufe sehen. Natürlich

sind die Daten anderer Arbeitgeber und Versicherten auch tabu. Der Broker dagegen darf nur auf die für die Angebotserstellung benötigten Funktionalitäten zugreifen. Also keine Daten von Versicherten und Arbeitgebern.

Der Informationssicherheit und den Sicherheitsbedürfnissen der Vorsorgeeinrichtungen ist damit aber noch nicht ausreichend Rechnung getragen. Hierfür müssen weitere Punkte erfüllt sein. Zum einen ist auf eine Multi-Factor-Authentication (MFA) zu achten. Das ist ein Anmeldeverfahren bei dem verschiedene Methoden zur Identifizierung des Users kombiniert werden. Dazu zählen zum Beispiel:
– Username
– Passwort
– Token
– Pin

Zum Verständnis: Der Versicherte authentisiert sich (Authentisierung) durch Eingabe von Username, Passwort, Token und möglicherweise weiterer Sicherheitselemente. Das System authentifiziert ihn als Versicherten (Authentifizierung – Wer bist du?). Der Versicherte ist dann autorisiert (Autorisierung – Was darfst du?) dies und jenes zu tun oder eben nicht. Die Verwendung der Multi-Factor-Authentication (MFA) hilft die Sicherheit massgeblich zu verbessern. Darüber hinaus gibt es aber weitere potentielle Schwachstellen, die beseitigt werden müssen.

Technische Risiken

Der Programmcode der Webapplikation kann Sicherheitslücken aufweisen. Hier spricht man dann zum Beispiel von SQL-Injection, Code-Injection, Log-Injection, Directory Traversal oder XML-Injection. Die SQL-Injection ist wohl die grösste Gefahr für die Datenintegrität. Insofern lohnt es sich hier näher darauf einzugehen. Beim Zugreifen der Anwendung auf die Datenbank, werden Befehle in Form von SQL-Anweisungen an die Datenbank übermittelt. Ist die Anwendung anfällig für SQL-Injection, kann ein Angreifer durch Manipulation der Eingabedaten geänderte oder zusätzliche SQL-Anweisungen injizieren, die von der Anwendung an die Datenbank weitergeleitet und dort bearbeitet werden. Auf diese Weise können wie bei einem direkten Datenbankzugriff beliebige SQL-Anweisungen ausgeführt werden und so Sicherheitsmechanismen der Anwendung beim Datenzugriff umgangen werden. Eine SQL-Injection kann sich beispielsweise wie folgt auswirken:
– Unberechtigter Zugriff auf Daten
– Erzeugen, Auslesen, Verändern oder Löschen von Daten
– Ausführen von Betriebssystembefehlen
– Kontrolle über die Datenbank
– Zugriff auf weitere Server

Um eine SQL-Injection zu verhindern, müssen sich die Softwareentwickler der Webanwendung an die entsprechenden Programmierregeln halten. Damit der unberechtigte Zugriff auf die Daten und allfällige Veränderungen durch SQL-Injection ausgeschlossen werden kann muss der Programmcode zusätzlich einem entsprechenden Review unterzogen werden. Um die Sicherheit noch zusätzlich zu erhöhen sollte die Web-Applikation sogenannten Penetrationstests durch ein spezialisiertes Unternehmen unterzogen werden.

Fehler minimieren

Um die Integrität der Daten im Versichertenverwaltungssystem zu gewährleisten und offensichtlich falsche Mutationen nicht zu übernehmen, braucht es zudem einen ausgeklügelten Mechanismus zur Plausibilisierung und Mutationsübernahme. Zudem muss die Nachvollziehbarkeit der Mutationen, sprich wer hat wann welche Änderung vorgenommen, sichergestellt sein.

Weitere Schwachstellen können server- und datenbankseitig auftreten. Um diese Sicherheitslücken zu schliessen, müssen auch hierfür geeignete Massnahmen getroffen werden. Wobei eine hundertprozentige Sicherheit sowieso nie erreicht wird. Als jüngeres Beispiel dafür steht die SSL-Sicherheitslücke Heartbleed bei dem ein grosser Teil des Internets betroffen ist.

Schliesslich bleibt den Vorsorgeeinrichtungen die Abwägung zwischen Nutzen und Risiko.