
Bildquelle: Peter H @Pixabay

WIE BERECHTIGUNGSSYSTEME DAS BANKGEHEIMNIS AUSHEBELN

Wer sich vor Kurzem beim schwedischen Bezahldienst Klarna eingeloggt hat, bekam womöglich die privaten Daten von fremden Leuten zu sehen.

Das ist vor etwas längerer Zeit auch Kunden von comdirect passiert. Nicht immer stecken Hacker hinter solchen Datenpannen. Häufig hakt es in den IT-Systemen selbst.

In der digitalen Welt lautet die wichtigste Frage, die sich für einen beliebigen Dienst stellt: Darf der das überhaupt? Die IT-Systeme müssen beispielsweise feststellen, dass Frau Meier wirklich Frau Meier ist, bevor sie im Online-Banking ihre Kontodaten anzeigen – und vorher abgleichen, ob sie sich nicht als Mitarbeiterin einloggt. Davon hängen die Berechtigungen ab, die sie bekommt. Viele Banken unterschätzen, wie komplex diese Regeln mitunter sind, und geraten ins Stolpern, wenn sie ihre Software aktualisieren, ihre digitalen Angebote erweitern oder Systeme harmonisieren, etwa nach einer Fusion.

Sechs goldene Regeln

Zu den besonders kritischen Fehlerquellen zählen Berechtigungen, die nicht einheitlich im IT-System abgebildet sind. Eine Bank ordnet beispielsweise Berechtigungen, Vollmachten und Limite einem Kundenstammvertrag zu. Bei der anderen hängen diese Informationen am Produkt, also etwa am Girokonto. Wer wissen will, ob er sein Überweisungslimit erhöhen darf, fragt technisch betrachtet im ersten Fall nach dem Vertrag und im zweiten nach dem Produkt. Wenn sich jetzt etwas am System ändert, wird es knifflig. Will die eine Bank die andere übernehmen, muss sie deren Rechteschema sauber in das eigene Modell überführen.

Ärger ist auch dann vorprogrammiert, wenn über verschiedene Schnittstellen Berechtigungen übermittelt werden – und im kommenden Open-Banking-Zeitalter dürfte das ständig passieren. Wer nicht aufpasst, muss verschiedene Wege zum Ziel berücksichtigen und nimmt neben einem unübersichtlichen API-Design auch in Kauf, dass kleine Änderungen zu Fehlern führen. Damit das nicht passiert, schreiben viele Institute zusätzliche Anforderungen in das Berechtigungssystem. Doch damit schaffen sie sich nur einen unbändigen Monolithen, den sie mit großem Aufwand pflegen müssen. Sechs Regeln helfen dabei, das zu vermeiden:

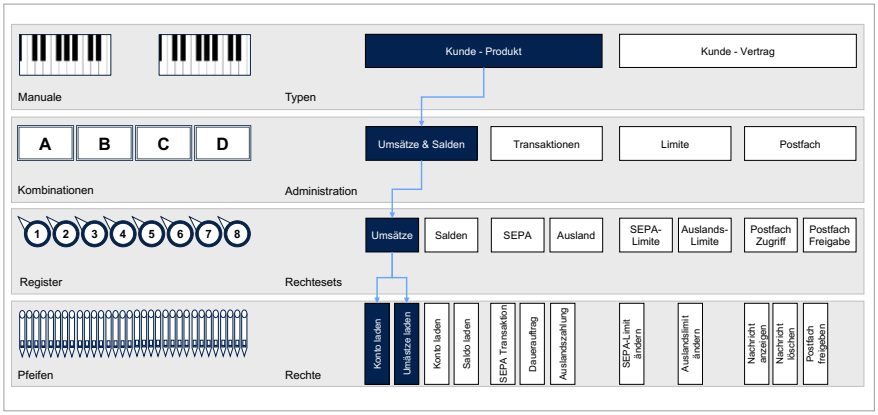
Engen Scope festlegen: Ins Berechtigungssystem kommt nur, was auch tatsächlich mit Rechten zu tun hat. Nicht dazu gehören Produkt-Features, etwa dass Sparkonten keine Auslandsüberweisungen erlauben. Menschen leuchtet das ein, einer Maschine muss man das aber beibringen.

Redundanzen eliminieren: Keine doppelten Prüfungen übernehmen. Viele historisch gewachsene Systeme leiten konkrete Berechtigungen noch aus Rollen und zusätzlich aus einem Berechtigungssystem ab. Das muss nicht sein.

Separationen strikt einhalten: Prüfungen und Abhängigkeiten sollten sich gegenseitig nicht bedingen. Beispiel: Berechtigungen eines Nutzers an einem Produkt dürfen nicht auch noch davon abhängen, welcher Kundengruppe dieser angehört.

Einheitlichkeit sicherstellen: Das System bildet die Berechtigungen von Kunden, Mitarbeitern und technischen Benutzern identisch ab.

Programmierung von Fachlichkeit und Administration trennen. Beispiel: Granulare Berechtigungen, die sich für Fachlichkeit und Administration einzeln konfigurieren lassen, statt sie zusammenzufassen.



Vorbild Kirchenorgel: Berechtigungen auf vier Ebenen Bildquelle: Senacor Technologies AG

Richtige Architektur wählen: Tokens, asynchrones Messaging und REST-APIs eignen sich, um Berechtigungen abzufragen und bekannt zu geben. Welche Methode am besten passt, sollte jedes Institut vorab genau prüfen.

Vorbild Kirchenorgel

Damit das Berechtigungssystem trotz dieser sechs Regeln flexibel bleibt, sollte das System alle Berechtigungen für jeden Geschäftsvorfall auf mehreren Ebenen abbilden. Dabei hat sich insbesondere bei komplexen oder wachsenden Berechtigungssystemen bewährt, vier Ebenen einzurichten und ihr Zusammenspiel zu organisieren wie bei einer Orgel in der Kirche. Auf der ersten Ebene stehen die Pfeifen, die den Ton erzeugen. Auf der zweiten Ebene arbeiten sogenannte Register, die regeln, welche Pfeifen tönen dürfen. Kombinationen dieser Register erleichtern, schnell zwischen wiederkehrenden Mustern zu wechseln. Verschiedene Manuale erlauben zudem, verschiedene Klänge zugleich abzubilden.

Ein wesentlicher Vorteil: Dieses Orgelsystem bildet verschiedene Arten von Berechtigungen identisch ab. Gleichzeitig lässt sich über Kombinationen für jeden Kunden einstellen, was er darf und was nicht. Mit der Fachabteilung wird der Schnitt der Register abgestimmt: „Konto laden“ und „Umsätze laden“ gehören beispielsweise zum Register Umsätze. So deckt das System die gesamte Bandbreite an Diensten einer Bank ab, so wie die Orgel das komplette Klangspektrum über die Pfeifen. Drückt der Organist aus Versehen die falsche Taste, erklingt den Zuhörern ein schiefer Ton – in diesem Bild führt ein falscher Ton, also die nicht korrekte Berechtigung dazu, dass die Pfeife stumm bleibt.

Rechte bekannt machen

Wer so weit gekommen ist, muss jetzt nur noch gewährleisten, dass alle verwendeten Dienste wissen, welche Rechte wann gelten. Hinzu kommt, dass die Systeme nicht immer auf dieselbe Art und Weise nach Berechtigungen fragen. Ein System möchte beispielsweise wissen, wer welche Dienste nutzen darf. Ein zweites, wer alles für einen Dienst freigeschaltet ist, und ein drittes, ob ein einzelner Dienst einer einzelnen Person zur Verfügung steht. Weil eine REST-Schnittstelle allein dafür bereits drei Endpunkte benötigt und sich deshalb schnell selbst zu einem Risiko entwickeln kann (siehe Kasten), eignet sich dafür asynchrones Messaging.

Der Vorteil von asynchronem Messaging: alle Systeme werten den gleichen Datensatz aus – und das unabhängig voneinander. Wenn sich etwas ändert, jemand etwa ein Wertpapierdepot eröffnet und deshalb neue Berechtigungen erhält, erzeugt das Berechtigungssystem dafür ein Ereignis. Alle betroffenen Umsysteme brauchen dann nur noch die jeweils für sie relevanten Ereignisse zu abonnieren und die empfangenen Daten auszuwerten. Will der Kunde jetzt eine Aktie kaufen, wissen diese Systeme bereits Bescheid und erlauben die Transaktion. So eine Lösung lässt sich leicht skalieren und gilt als wenig ausfallgefährdet.

Fazit: Ein durchdachtes Berechtigungssystem erspart einer Bank so manche Peinlichkeit. Wütende Kunden sind aber nicht der einzige Grund, warum sich gerade jetzt ein kritischer Blick hinter die Kulissen lohnt. Auch die Aufsicht interessiert sich dafür. In der aktuell konsultierten Fassung der BAIT spricht die Bafin davon, alle Ebenen der IT-Systeme, von der Datenbank über das Betriebssystem bis hin zu den Anwendungen (Tz. 6.2), in die Berechtigungssysteme einbeziehen zu wollen. Zudem muss die Bank sicherstellen, dass neu eingerichtete, geänderte sowie deaktivierte oder gelöschte Berechtigungen umgehend oder zumindest zeitnah in den Zielsystem nachvollzogen werden (Tz. 6.4). All das spricht für eine Extrameile, die Banken mit ihren Berechtigungssystemen gehen sollten – und für weniger Bildschirme, die hin und wieder zu nahe am Fenster stehen und so das Bankgeheimnis mitunter ganz altmodisch hintergehen.

DAS REST-RISIKO

Bei vielen verschiedenen Berechtigungen bieten REST-Schnittstellen einige Vorteile. Sie gelten aber auch als ein Single Point of Failure. Zu den Risiken zählen eine schwankende Auslastung, drohende Überlast und unterschiedliche Abnehmer, die sich jeweils andere Endpunkte wünschen. All das kann die REST-API anschwellen und schlimmstenfalls ausfallen lassen. Dann liegt das gesamte Banking lahm.

Autor: Severin Matthes

Senior Consultant bei Senacor Technologies