HANSER

Leseprobe

zu

Authentifizierung und Autorisierung in der IT

von Andreas Lehmann, Mark Lubkowitz und Bernd Rehwaldt

Print-ISBN: 978-3-446-47949-4
E-Book-ISBN: 978-3-446-48000-1
E-Pub-ISBN: 978-3-446-48001-8

Weitere Informationen und Bestellungen unter
https://www.hanser-kundencenter.de/fachbuch/artikel/9783446479494
sowie im Buchhandel

© Carl Hanser Verlag, München

Inhalt

Vorwort

The world's most valuable resource is no longer oil, but data.

Economist, 2017

„The world's most valuable resource is no longer oil, but data" ist die Titelzeile des Economist aus dem Jahr 2017. Sie hat sich mittlerweile zu „Data is the new oil" weiterentwickelt. Adressierte der Economist mit ihr ursprünglich das Monopol der dominierenden Firmen im Digitalmarkt, wird sie heute meist verwendet, um die Wertigkeit und das Potenzial von Daten hervorzuheben. Die Existenz einiger der weltweit wirtschaftskräftigsten Unternehmen basiert rein auf Daten. Allgemeiner gesagt: Daten sind heute längst einer der wichtigsten Rohstoffe jedes Unternehmens.

Dieser Rohstoff ist wertvoll.

Dieser Rohstoff ist schutzwürdig.

Dieser Rohstoff benötigt besondere Behandlung.

Der Verlust oder die Veröffentlichung von vertraulichen Daten kann einerseits erheblichen Schaden für ein Unternehmen verursachen. Umfassen diese Daten andererseits personenbezogene Informationen, dann folgen auch strafrechtliche Konsequenzen mit teils empfindlichen Geldstrafen.

Lagerten Werte früher häufig in Tresoren, werden sie heute beinahe ausschließlich in IT-Systemen aufbewahrt. Ein Tresor schützt seinen Inhalt etwa durch Wissen in Form einer Zahlenkombination, Besitz in Form eines Schlüssels oder beides. Wer die Zahlenkombination kennt oder den Schlüssel besitzt, konnte sich autorisieren und auf den Inhalt des Tresors zugreifen. Eine Authentifizierung, also wer den Tresor öffnet, war nicht nötig.

Anders sieht es bei IT-Systemen aus. Um in IT-Systemen verarbeitete Daten angemessen zu schützen, müssen drei Ziele erreicht werden: Vertraulichkeit, Integrität, Verfügbarkeit.

- **Vertraulichkeit:** Die Daten sind nur den Personen und Systemen zugänglich, die diese zur Erfüllung ihrer jeweiligen Tätigkeit benötigen.
- **Integrität:** Die Daten sind inhaltlich korrekt und Änderungen nachvollziehbar.
- **Verfügbarkeit:** Die Daten sind gegen Löschen und sonstigen Verlust des Zugriffs gesichert.

Erreichen lassen sich diese drei Ziele, indem sich jede zugreifende Person und jedes zugreifende System authentifizieren und autorisieren müssen.

Welche Maßnahmen zum Schutz von Daten dafür heutzutage in Frage kommen und was es dabei zu beachten gilt, das ist Inhalt dieses Buches.

München, Januar 2024

Andreas Lehmann, Mark Lubkowitz, Bernd Rehwaldt

2 Anwendungsfälle

As we've come to realize, the idea that security starts and ends with the purchase of a prepackaged firewall is simply misguided.

Art Wittmann

Warum Authentifizierung und Autorisierung in der IT heute ein entscheidender Faktor sind, lässt sich kurz und knapp mit dem hohen Geschäftswert von Daten beantworten. Außerdem mit dem Umstand, dass IT-Systeme im täglichen Geschäftsbetrieb unverzichtbar sind.

Offen ist die Frage: Wann sind Authentifizierung und Autorisierung relevant?

Die kurze und knappe Antwort: Jedes Mal, wenn der Zugriff auf Daten und Systeme erfolgen soll. Diese Situationen lassen sich in acht verschiedene Anwendungsfälle unterscheiden. Bei einigen Anwendungsfällen scheinen die Unterschiede eher geringfügig zu sein und fallen im ersten Moment nicht auf. Bei anderen ist der Unterschied sofort ersichtlich.

Die nachfolgenden Anwendungsfälle beschreiben daher stets eine eindeutige Ausgangssituation. Dazu gehört etwa, ob ein Anwender mit einem vertrauenswürdigen Client oder einem nicht-vertrauenswürdigen Client zugreifen möchte, ob der Anwender Informationen teilen oder auf Ressourcen zugreifen möchte, ob sich der Anwender mit einem allgemeinen Profil oder einem speziellen Profil authentifizieren möchte und Ähnliches.

2.1 Vertrauenswürdiger Client

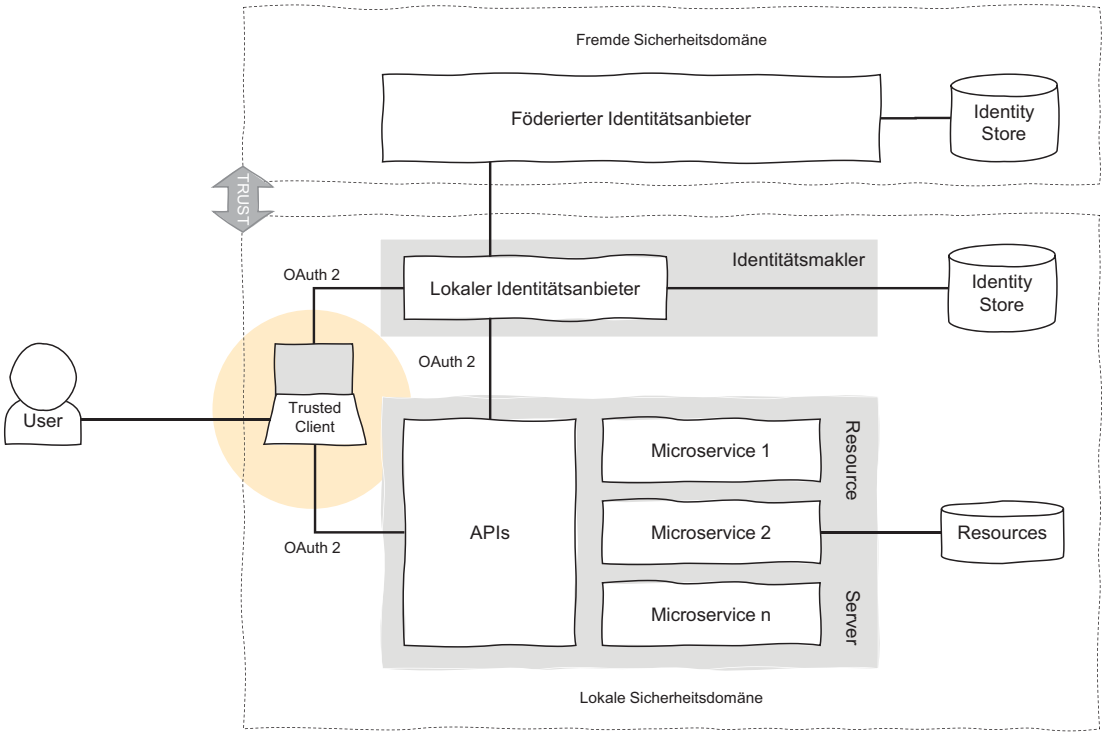

Bild 2.1 Vertrauenswürdiger Client: Der Anwender greift mit einem vertrauenswürdigen Client zu.

Einer der am häufigsten anzutreffenden Anwendungsfälle ist der Zugriff eines Anwenders mit einem vertrauenswürdigen Client. Dieser ist im Unternehmenskontext alltäglich. Bild 2.1 stellt diesen Anwendungsfall in der Übersicht dar.

Der Ausgangspunkt ist, dass der Anwender auf ihm gehörende oder ihm zugeordnete Ressourcen zugreifen möchte und dafür einen vertrauenswürdigen Client nutzt. Dieser Client gehört zur lokalen Sicherheitsdomäne, etwa eines Unternehmens.

Die Ressource selbst wird durch einen Microservice bereitgestellt, der wiederum durch eine API abgesichert ist. Auch die API ist geschützt respektive der Zugriff auf die API. Hierfür kommt ein lokaler Identitätsanbieter zum Einsatz. Der Zugriff auf die Ressource erfolgt also nicht direkt, sondern über mehrere Zwischenschritte, die die Sicherheitsrichtlinien umsetzen. Der Resource Server, der den Zugriff auf die Ressource schützt, prüft dann per OAuth Introspection das Token beim Identitätsanbieter auf Gültigkeit.

Mit OAuth, siehe Abschnitt 4.5, lässt sich dieser Anwendungsfall hervorragend absichern. Dabei bieten sich gleich drei verschiedene Grant Types an:

- *Authorization Code Grant Type*, beschrieben in Abschnitt 4.5
- *Resource Owner Credentials Grant Type*, beschrieben in Abschnitt 4.5
- *Client Credentials Grant Type*, beschrieben in Abschnitt 4.5

Das Bild 2.1 zeigt auch eine fremde Sicherheitsdomäne, die aber nicht in jedem Anwendungsfall vorkommen muss. Der Identitätsmakler dient in diesem Fall dazu, zwischen Identitätsanbietern einer lokalen und einer fremden Sicherheitsdomäne zu vermitteln. Wichtig ist dabei, dass zwischen der lokalen und der fremden Sicherheitsdomäne eine Vertrauensbeziehung bestehen muss.

2.2 Single Page Application

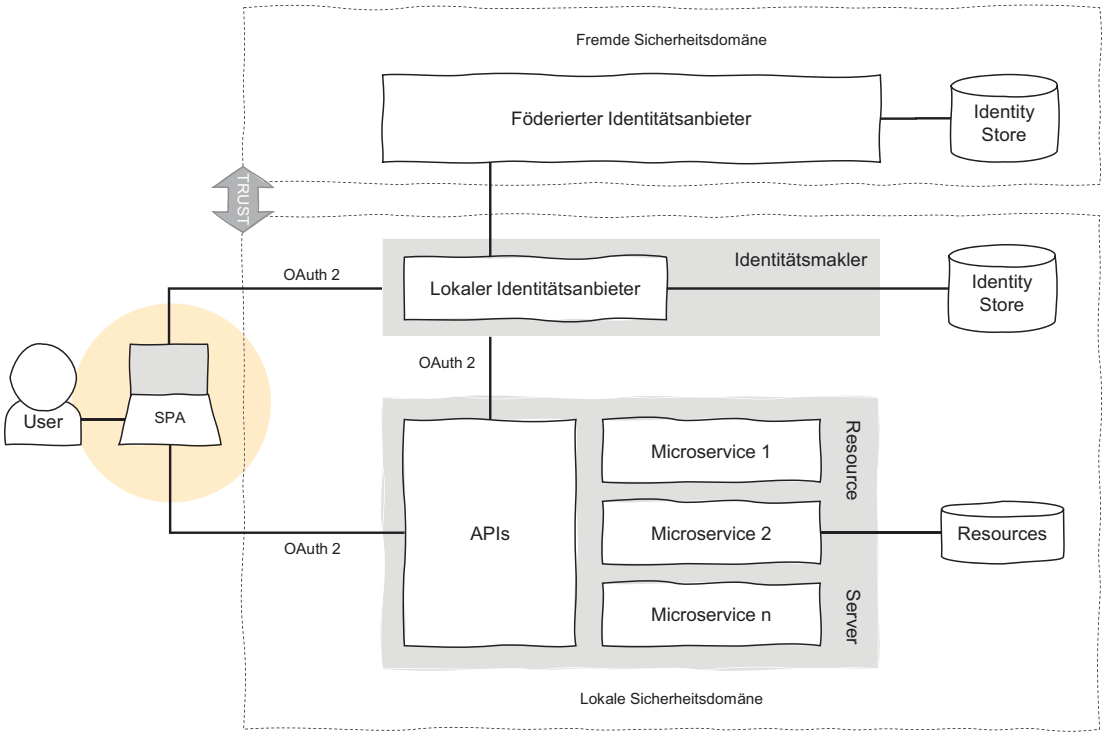

Bild 2.2 Single Page Applications: SPAs gelten generell als nichtvertrauenswürdige Clients. Grund ist, dass sich Code und Speicherbereich meist problemlos einsehen lassen.

Stichwortverzeichnis

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X

Y