Security

Web Engineering

Prof. D. König

Why Do We Care?

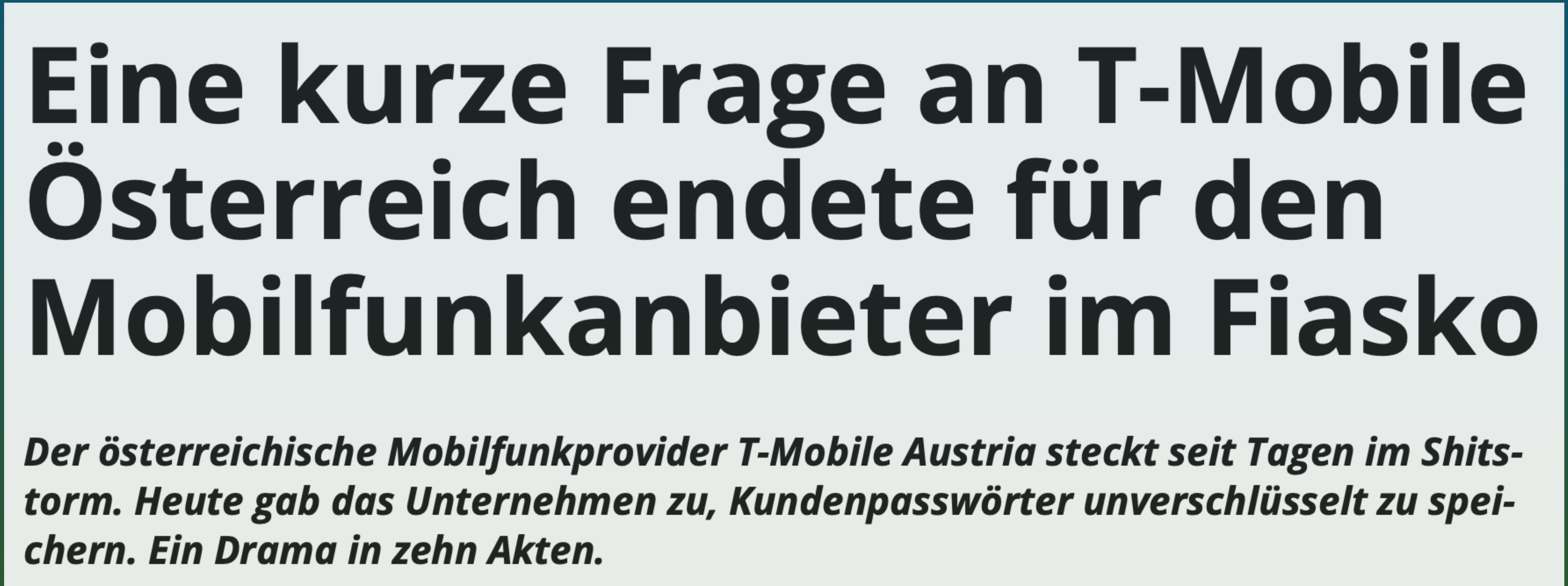
Often, for good UX and plain functionality, we need to *identify the user*.

But then…

With identification come further issues:
safe password management
user-creation denial of service attacks
lost passwords, revoking credentials, …

use of external service (OAuth) ?

What can go wrong?



Eine kurze Frage an T-Mobile Österreich endete für den Mobilfunkanbieter im Fiasko

Der österreichische Mobilfunkprovider T-Mobile Austria steckt seit Tagen im Shitstorm. Heute gab das Unternehmen zu, Kundenpasswörter unverschlüsselt zu speichern. Ein Drama in zehn Akten.

Keep it simple

There is *much* to know about security.

We need a *simple* initial introduction.

Let's follow best practices and use
Spring Security

Access Control

Once I can identify the user, I often want to restrict access based on the user's characteristics (guest, regular, admin)

Some Concepts

Authentication: who am I ?

Authorization: what am I allowed to do?

Principal, Role, Authority, Credentials,…

Strategies

Shield resource vs shield access path,

Allow all, shield selectively

Disallow all, open up selectively

Full Security

… is a topic that expands much more than what we can cover here.
Attend specialized modules.

We do a bare-bones introduction,
so let's start!