Mobile Application Security

Angriff von unterwegs

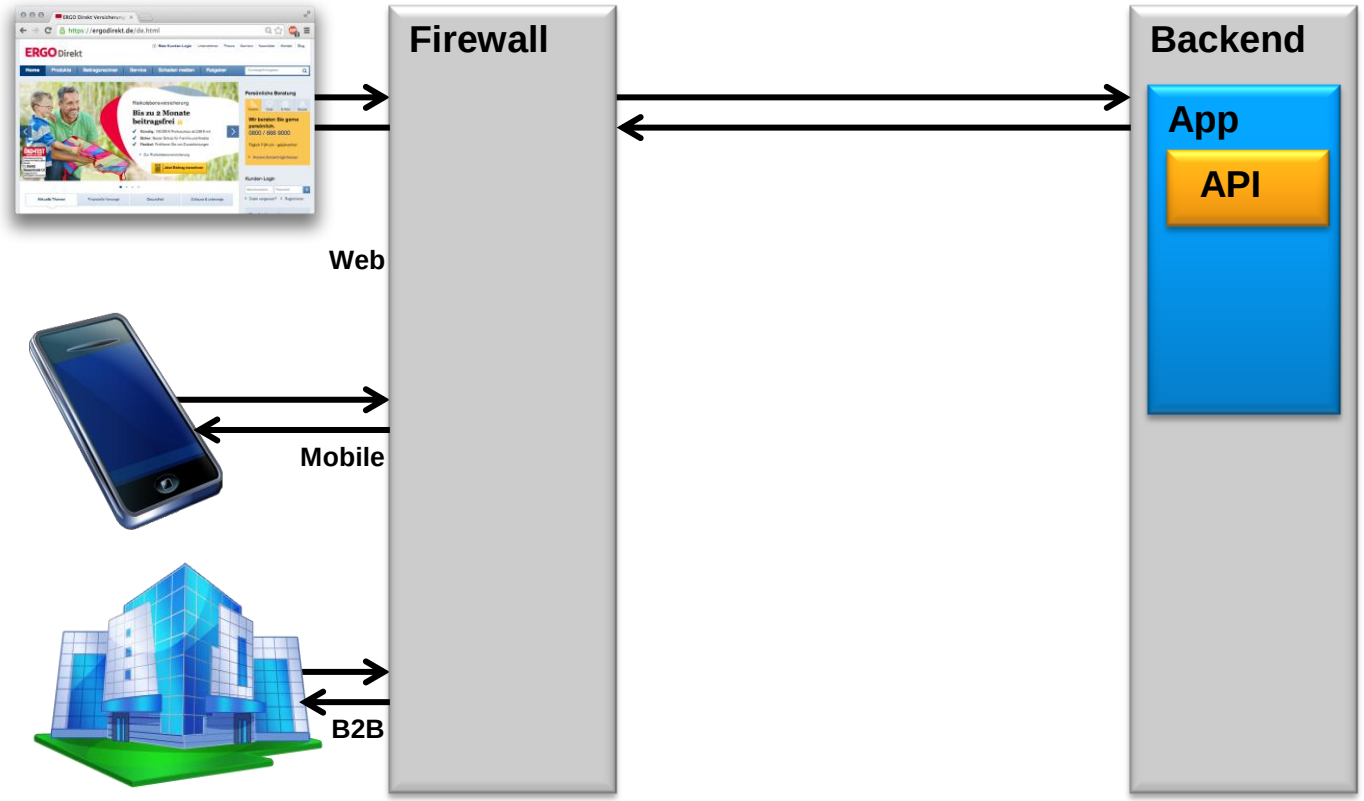
Tobias Polley (polley@predic8.de)
Thomas Bayer (bayer@predic8.de)

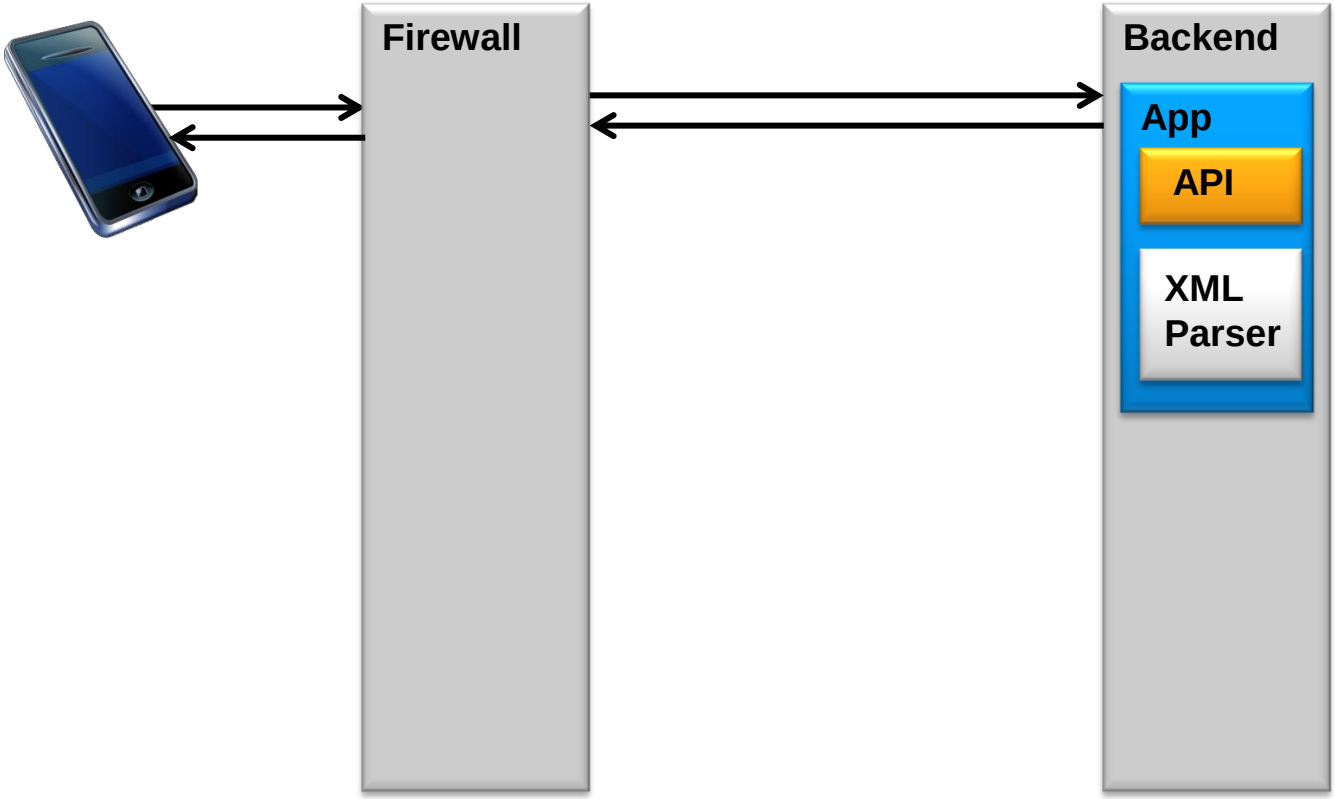
predic8 GmbH
Moltkestr. 40
53177 Bonn
predic8.de

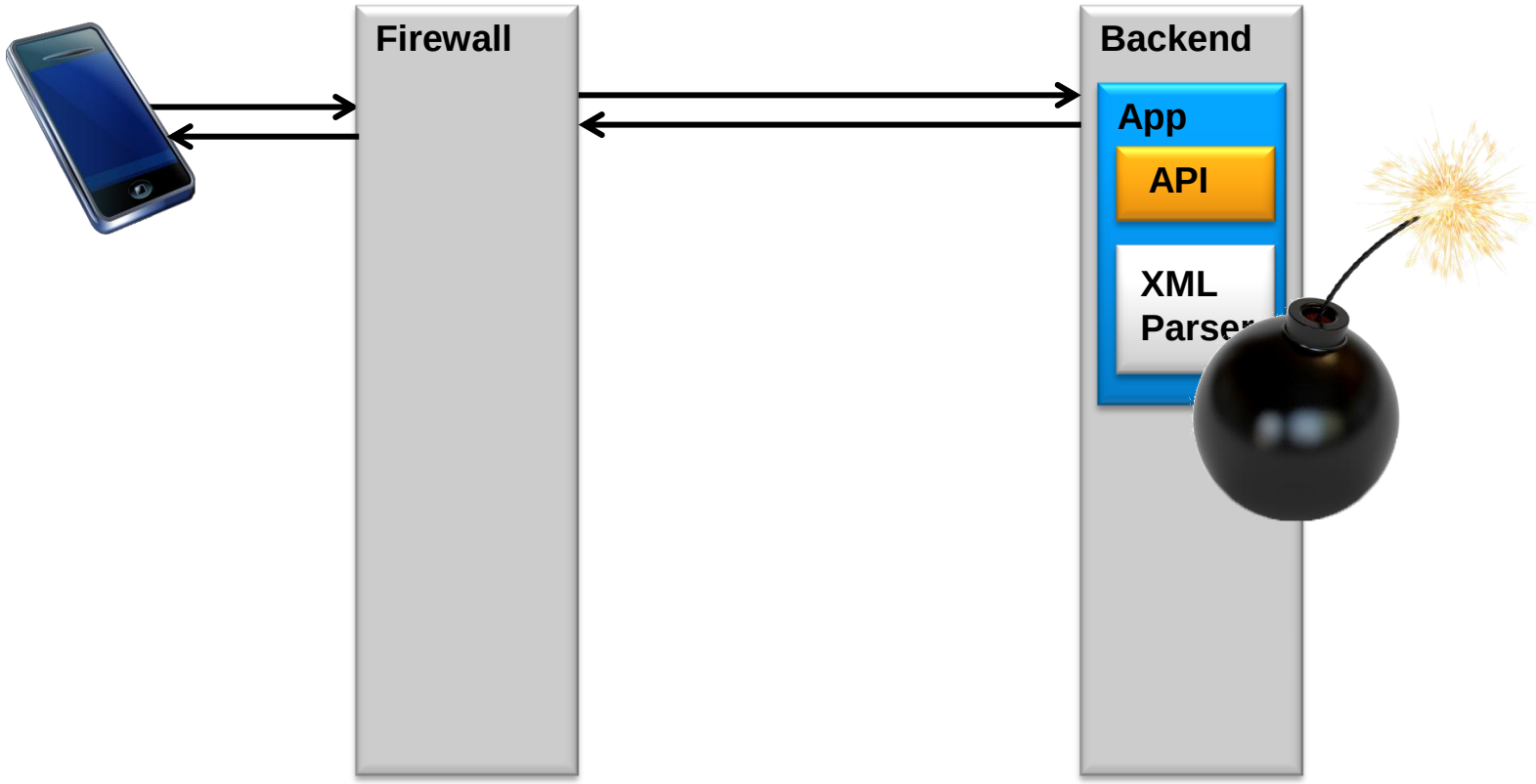
Agenda

- Ziele
- Angriff
- Schutz
- Case Study: Ergo Direkt Versicherungen

Web API




Firewall
Backend
App
API
XML
Parser


Firewall
Backend
App
API
XML

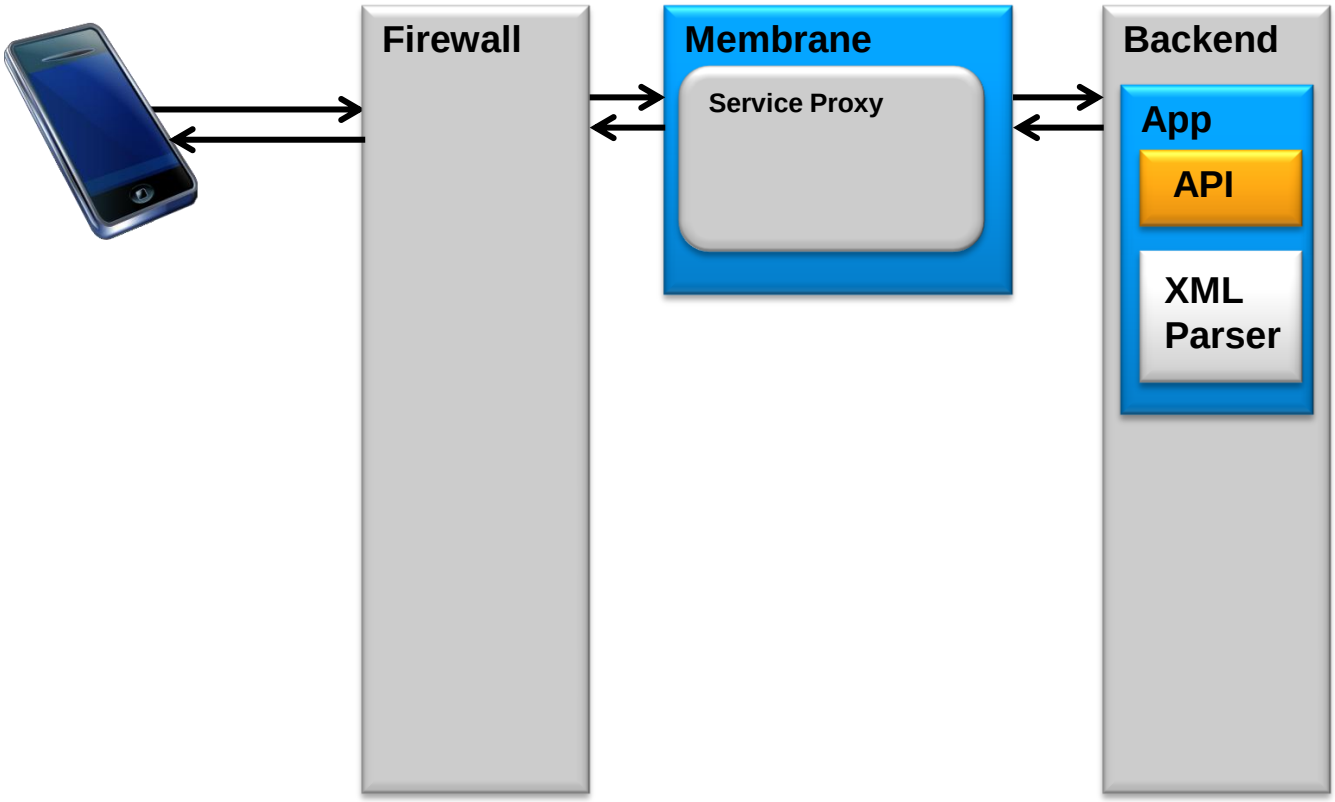
```
<?xml version="1.0"?>
<!DOCTYPE lolz [
 <!ENTITY lol "lol">
 <!ELEMENT lolz (#PCDATA)>
 <!ENTITY lol1 "&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;">
 <!ENTITY lol2 "&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;">
 <!ENTITY lol3 "&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;">
 <!ENTITY lol4 "&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;">
 <!ENTITY lol5 "&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;">
 <!ENTITY lol6 "&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;">
 <!ENTITY lol7 "&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;">
 <!ENTITY lol8 "&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;">
 <!ENTITY lol9 "&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;">
]>
<lolz>&lol9;</lolz>
```

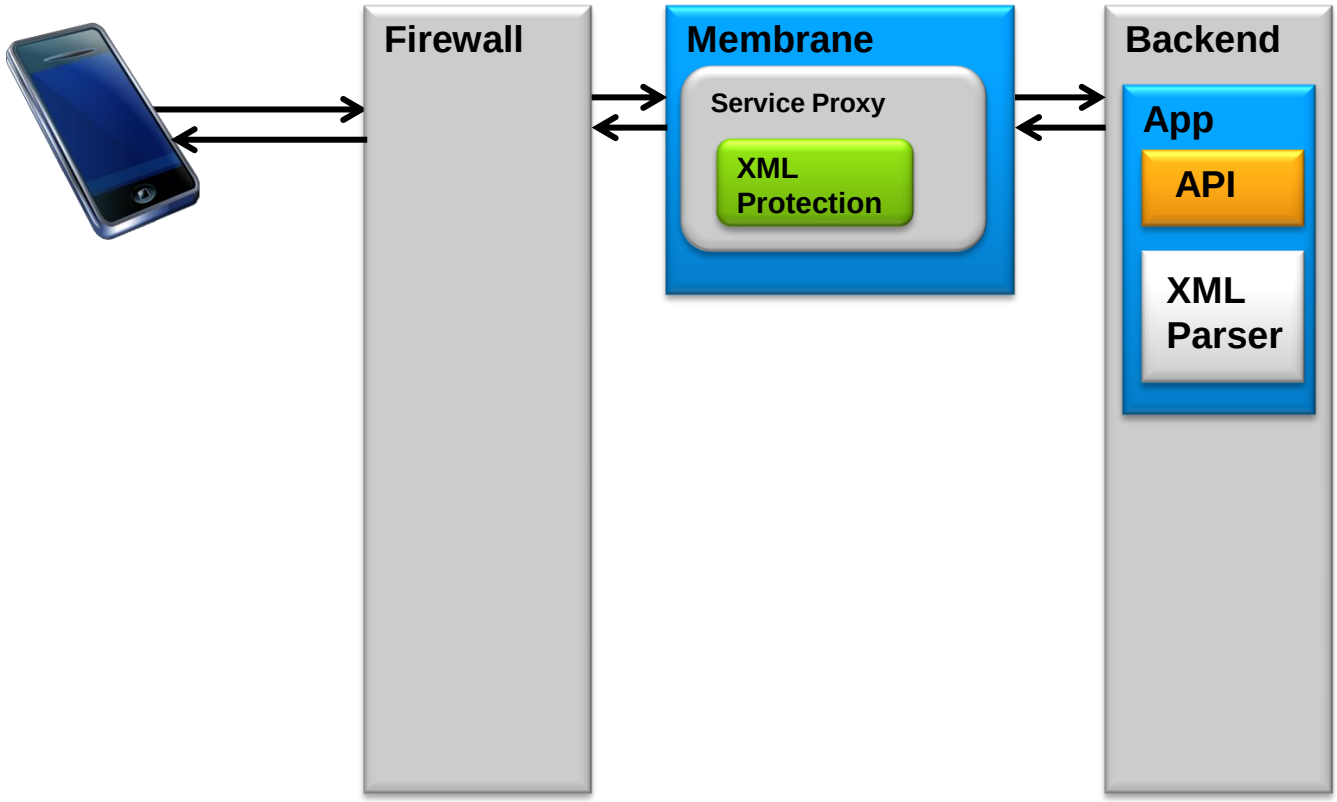
```
<?xml version="1.0"?>
<!DOCTYPE lolz [
 <!ENTITY lol "lol">
 <!ELEMENT lolz (#PCDATA)>
 <!ENTITY lol1 "&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;">
 <!ENTITY lol2 "&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;">
 <!ENTITY lol3 "&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;">
 <!ENTITY lol4 "&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;">
 <!ENTITY lol5 "&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;">
 <!ENTITY lol6 "&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;">
 <!ENTITY lol7 "&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;">
 <!ENTITY lol8 "&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;">
 <!ENTITY lol9 "&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;">
]>
<lolz>&lol9;</lolz>
```

```
<lolz>&lol9;</lolz>
```

```
<lolz>&lol8;&lol8;&lol8;&lol8;&lol
8;&lol8;&lol8;&lol8;&lol8;&lol8;
</lolz>
```

```
<lolz>
&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;
&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;
&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;
&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;
&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;
&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;
&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;
&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;
&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;
&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;
</lolz>
```

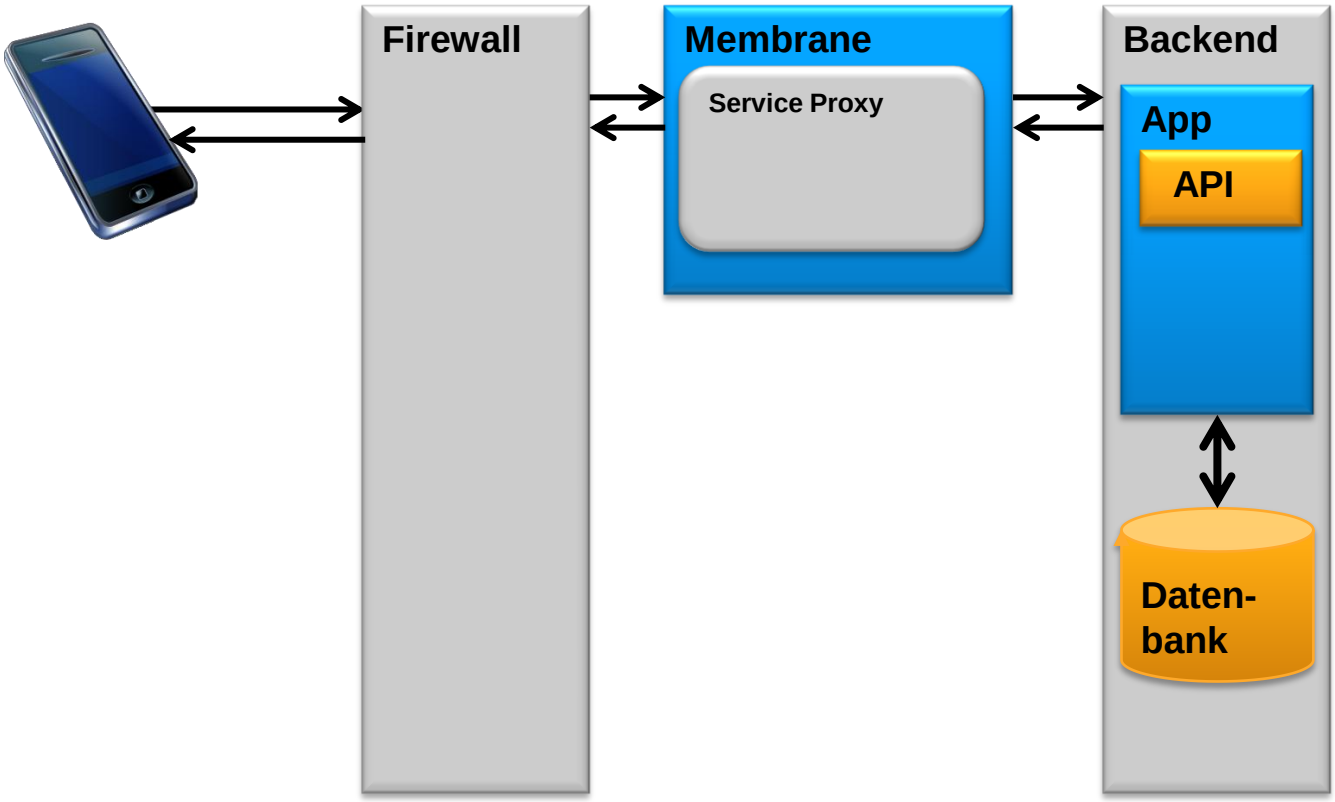

Firewall
Membrane
Service Proxy
Backend
App
API
XML
Parser


Firewall
Membrane
Service Proxy
XML Protection
Backend
App
API
XML Parser

predic8

1


TDS


Firewall
Membrane
Service Proxy
Backend
App
API
Daten-
bank

```
"SELECT id FROM usernames
WHERE name = '" + user +
"' and password = '" + password +
"';"
```

```
“SELECT id FROM usernames
WHERE name = ‘peter' and
password = ’pan';”
```

Demo

predic8

```
“SELECT id FROM usernames
WHERE name = 'peter' and
password = '' or '1' = '1';”
```

predic8

Vertraue keiner Eingabe!

Ablauf einer Attacke?

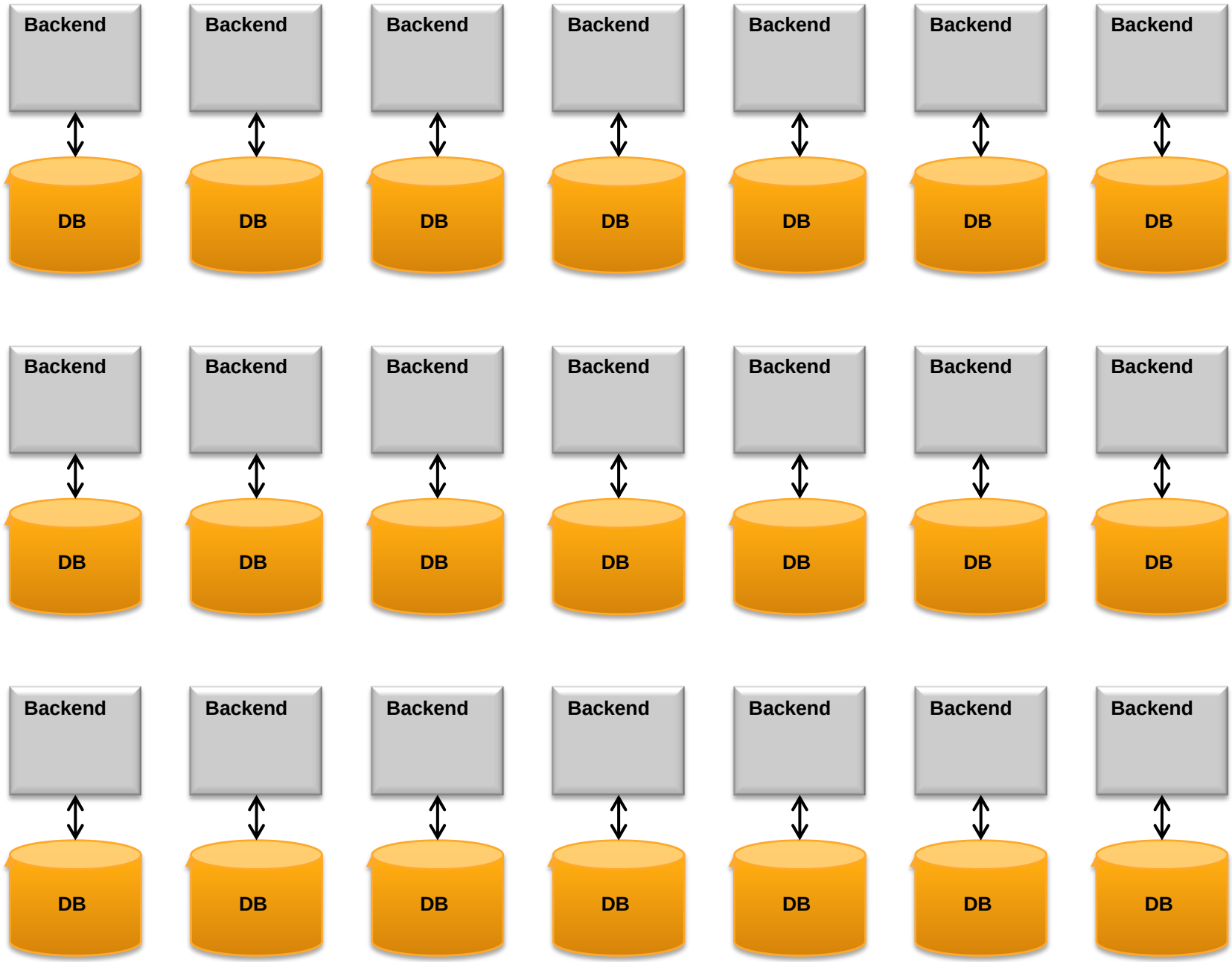
1. Intelligence
2. Zugang
3. Angriff
4. Einfluss

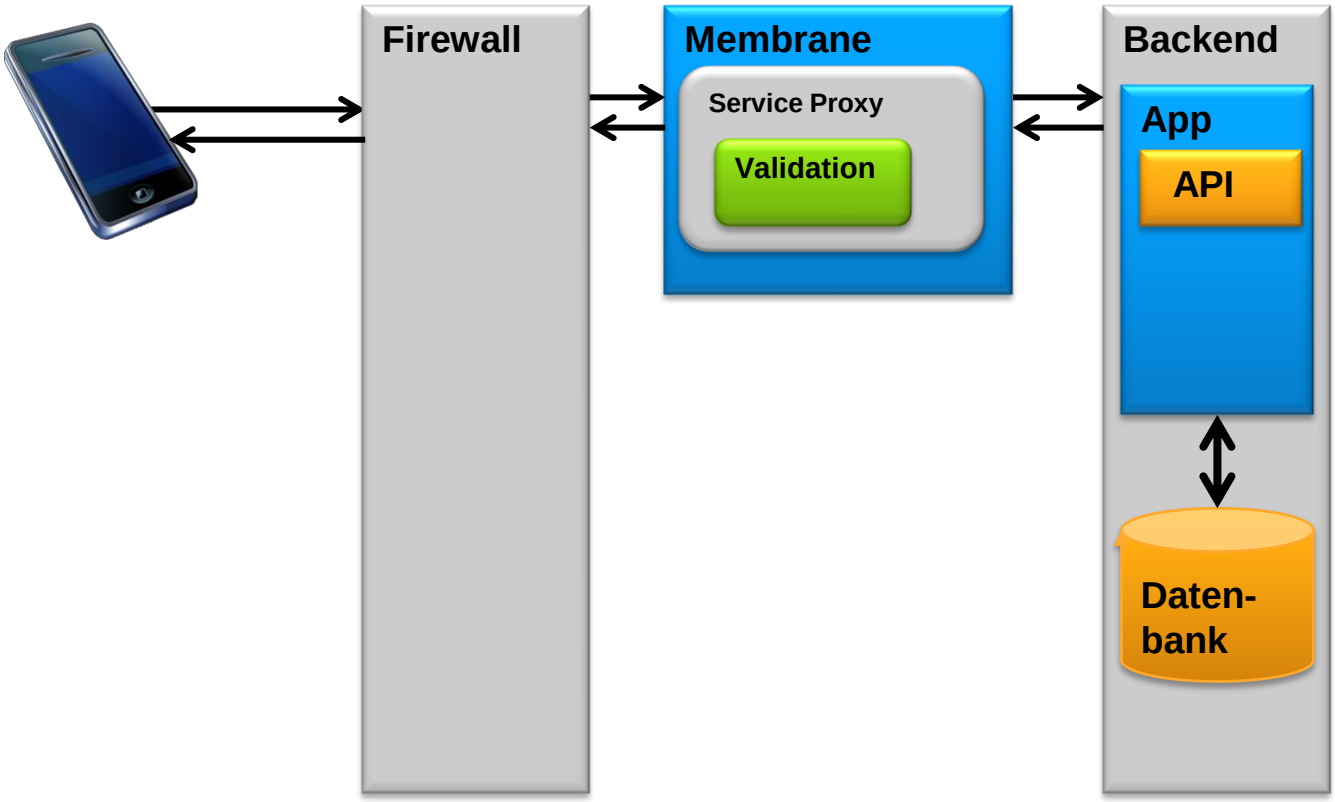
Was kann ein Angreifer tun?

- Informationen auslesen
- Löschen
- User anlegen
- Passwörter ändern
- Daten manipulieren
- Rechenzeit stehlen

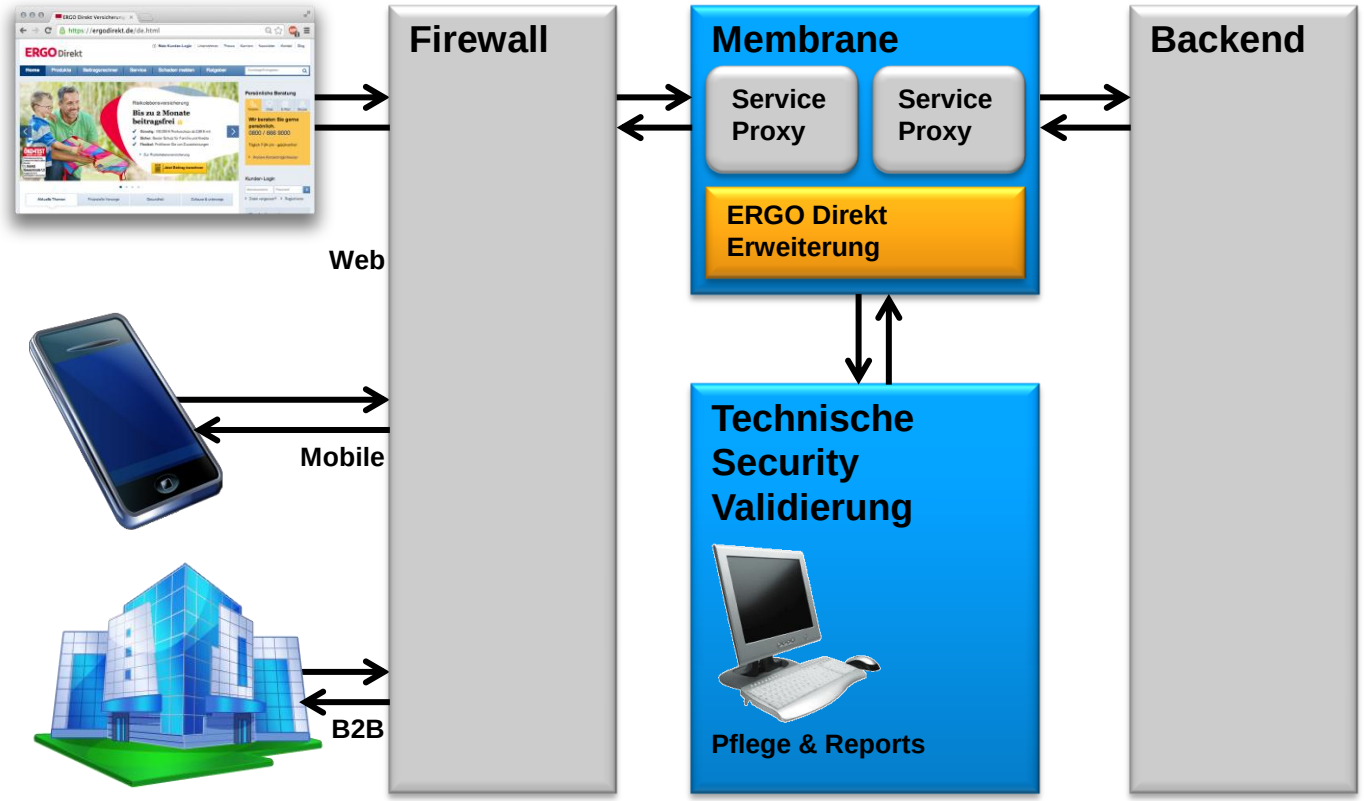
Vorkompiliertes SQL

```
"SELECT id FROM usernames
WHERE name = ? and password = ?;"
```


Backend
DB


Firewall
Membrane
Service Proxy
Validation
Backend
App
API
Daten-
bank

Demo


Firewall
Membrane
Service Proxy
Service Proxy
ERGO Direkt Erweiterung
Backend
Web
Mobile
B2B
Technische Security Validierung
Pflege & Reports

predic8

Apps brauchen Zugang zum Backend

Backends brauchen Schutz

predic8

Tobias Polley, polley@predic8.de
Thomas Bayer, bayer@predic8.de
www.predic8.de
www.membrane-soa.org

Bildnachweise

http://www.istockphoto.com/vector/warning-attention-sign-yellow-triangular-shape-black-exclamation-mark-pictogram-24334588

http://www.istockphoto.com/photo/syringe-and-vaccination-11003167

http://www.istockphoto.com/photo/bomb-in-old-style-with-a-burning-wick-11647534

http://www.istockphoto.com/photo/dynamic-duo-4413676