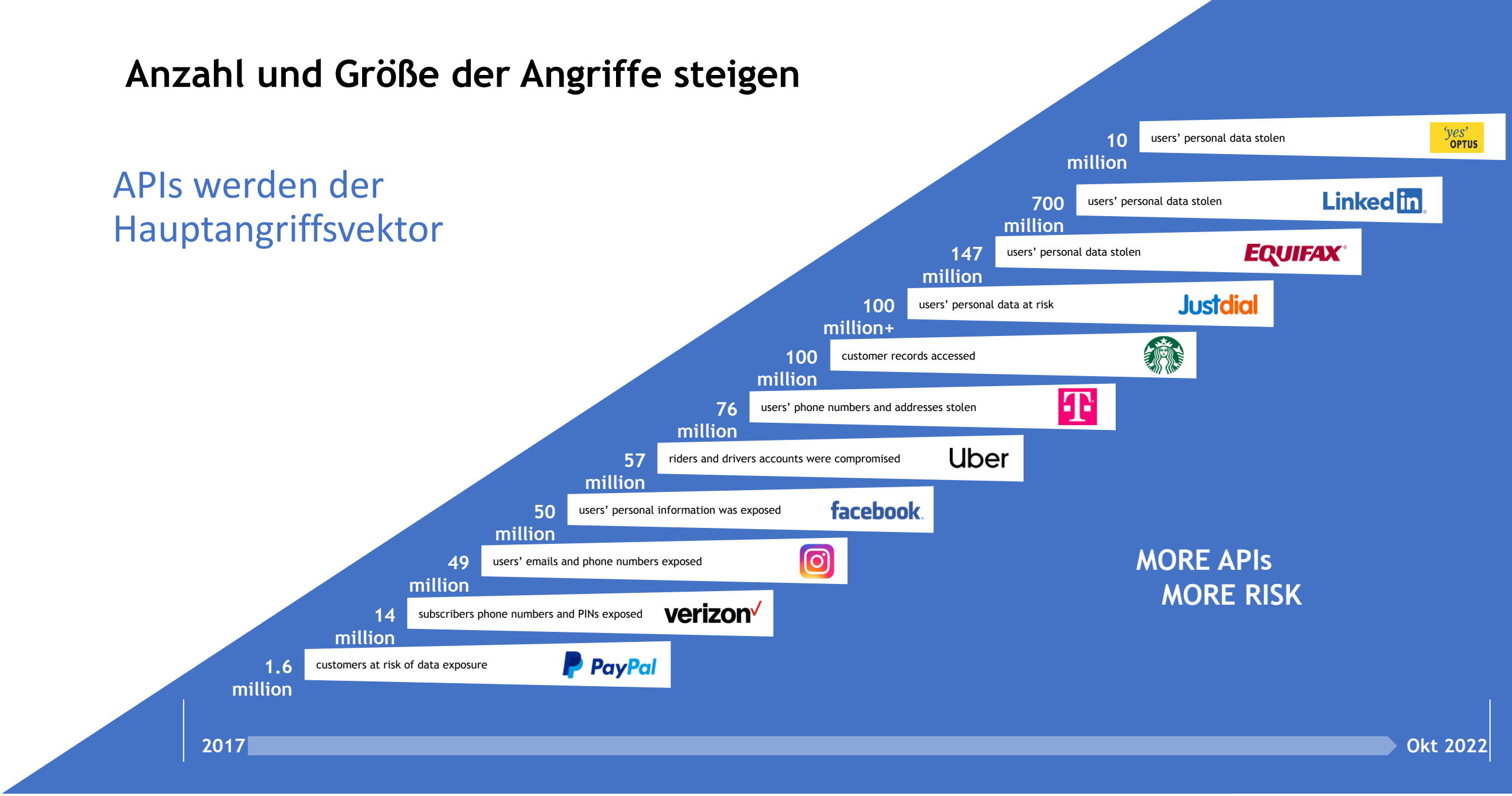
# Grundlegende Gedanken zu Sicherheit in der API Welt

Modul 1

# Anzahl und Größe der Angriffe steigen

## APIs werden der Hauptangriffsvektor



# Optus: Telekom in Australien


**Sicherheitslücke**

- Public API ohne Authentifizierung
- PII Daten unverschlüsselt
  - Pass/Führerschein Nr
  - Adresse
  - Geburtsdatum
  - TelefonNr
- Nutzennummer waren seriell in der URL

**Einordnung**

- 10 Millionen Datensätze entspricht ca. 40% der Bevölkerung Australiens
- Mit den Daten lässt sich sehr einfach **Identitätsdiebstahl** erstellen.
- **Folgeeffekte** des Datendiebstahls sind schon sichtbar (nach einem Monat)

source: https://www.upguard.com/blog/how-did-the-optus-data-breach-happen

# Es ist immer eine gefährliche Umgebung

# SECURITY LAYERS
## DEFENSE IN-DEPTH

1 **NETWORK LAYER SECURITY**
Firewalls, IDS/IPS, DMZ, Port scanners, network sniffers, patching, vulnerability scanners

2 **PLATFORM LAYER SECURITY**
Antivirus programs, patching, security specs for systems, access mgmt. & port scanning

3 **APPLICATION LAYER SECURITY**
Secure coding practices, Web Application firewalls, secure web gateway services.

4 **DATA LAYER SECURITY**
Encryption, User access and Identity Management, update systems.

5 **RESPONSE LAYER MECHANISM**
Security Monitoring, Intrusion detection, recovery.

Hier sind wir jetzt

# Grundlagen

**Burg mit Wassergraben**

- **Klare Grenzen**
- **Eindeutiger Eingang**
- **Klare Schutzmechanismen**

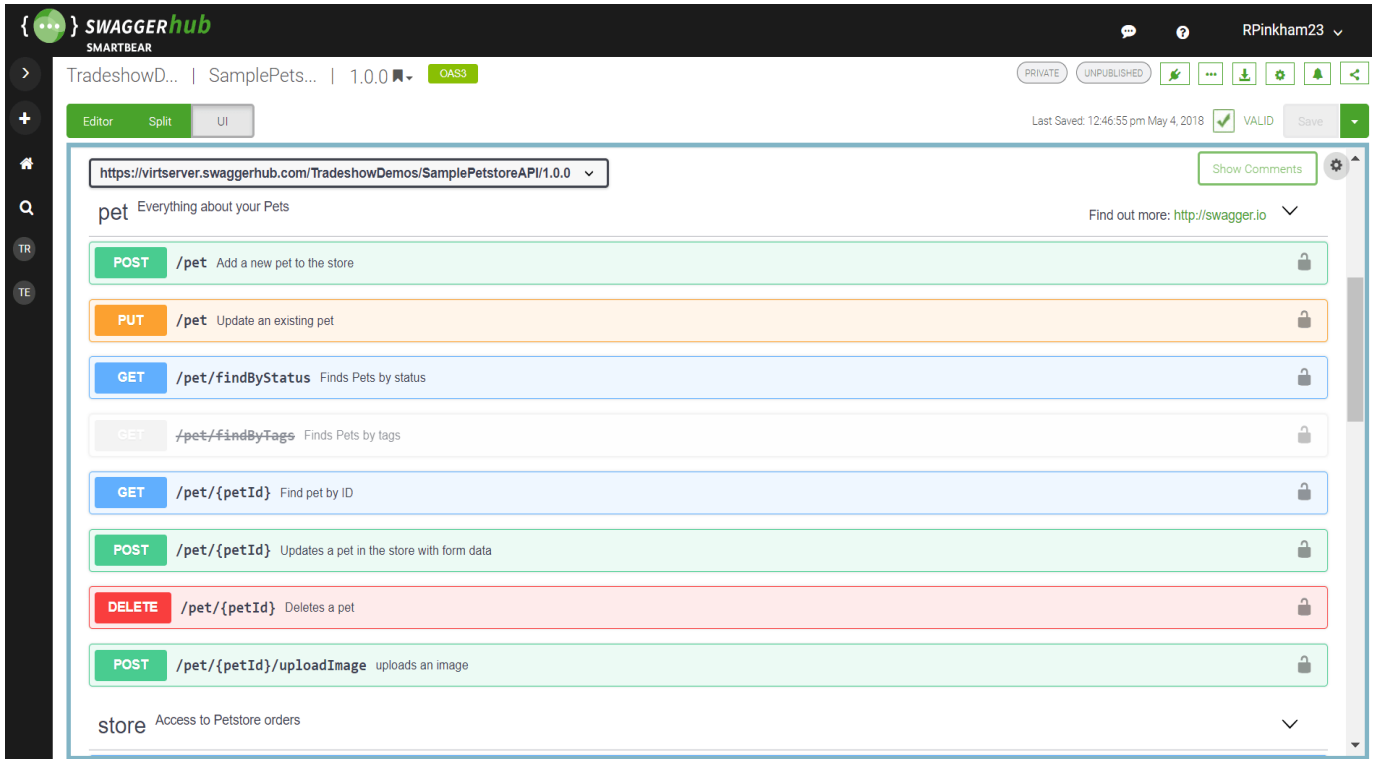
# Sicherheit im API Kontext

**Hauptkriterien die API Sicherheit von Applikations Sicherheit unterscheiden**

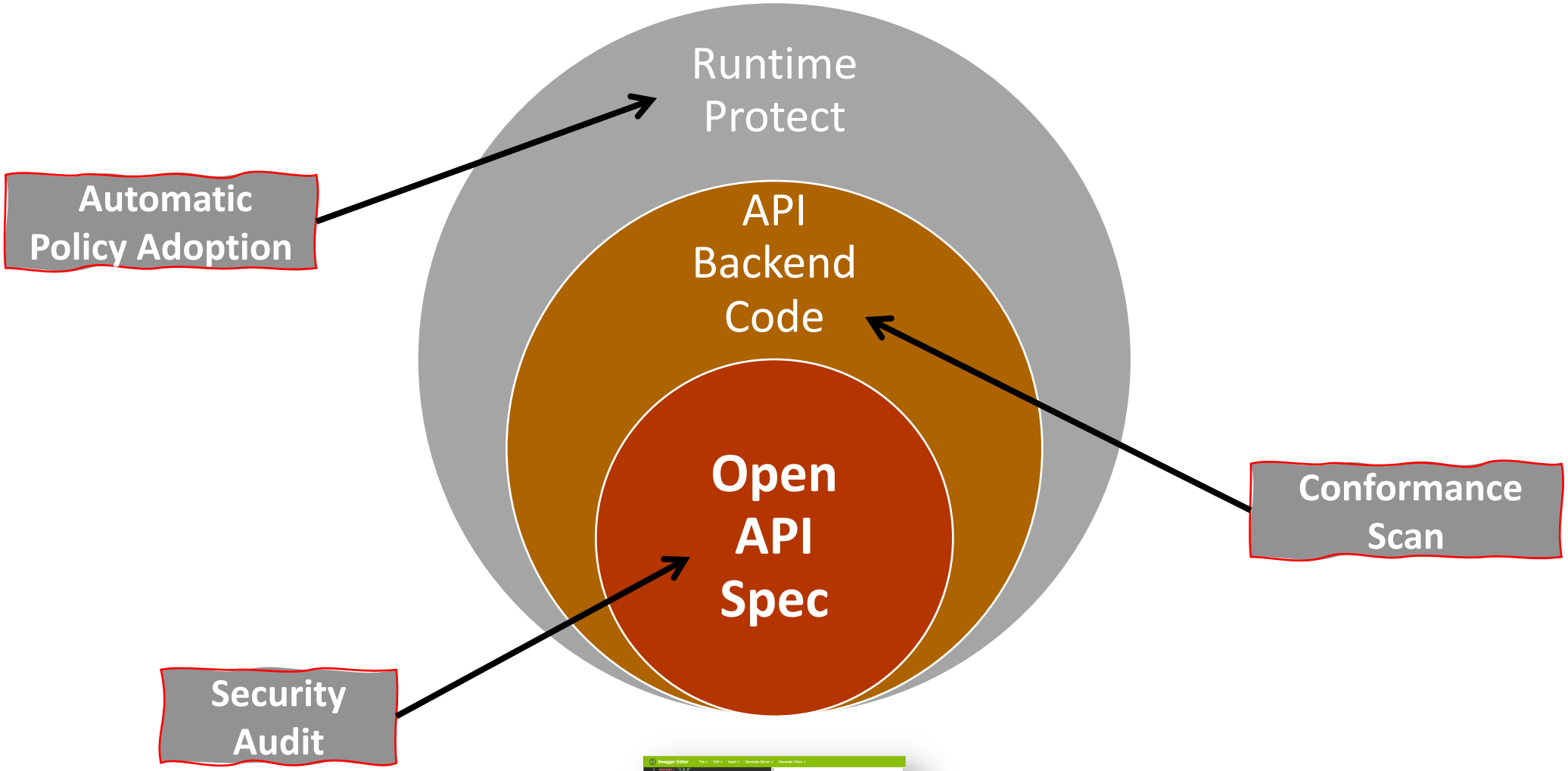
- **Eine Burg mit vielen Eingängen und keinem Graben**
- **Ein Browser ist nicht der Typische Nutzer der API**
- **Der Pfad ist nicht einfach eine Erweiterung der Ordnerstruktur**
- **Um Angriffe zu erkennen reicht es nicht nur die ankommenden Requests zu scannen.**

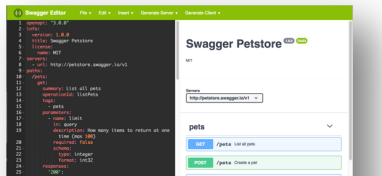
# APIs sind ein leichtes Ziel

- Sie sind einfach zu finden
- Sie sind gut dokumentiert
- Angriffe lassen sich leicht automatisieren
- Es gibt super Werkzeuge um die Angriffe zu automatisieren.



# Die Open API Spezifikation ist der Kern der Sicherheit



# Die Vorteile eines Positive Security Model

## Allowlist

- Allowed data types strong defined and enforce in OAS mode
- Data format can be precisely defined
- Operations can be fully specified too

- **Only allow data conforming to specification — anything else is an error**
- **Only allows “known good”**

VS.

## Blocklist

- Attempts to interpret data based on the runtime context i.e., Javascript, HTML
- Attempt to block what shouldn’t be present in a given context
- Can easily be subverted with encoding, etc.

- **Attempts to block “known bad”**

# Das ganze Bild