Kurzübung API-Sicherheit

Ergebnis vom 13.06.2019

Kurzübung API Sicherheit

Themenübersicht (25 min Bearbeitung in Teams zu 3-4 Studenten)

Team 1 - Einsatz von Token zur Zugriffskontrolle

Team 2 - Einsatz von Verschlüsselung und Signaturen

Team 3 - Identifizierung von Schwachstellen

Team 4 - Einsatz von Quotas und Throttling

In Anlehnung an: https://www.redhat.com/de/topics/security/api-security

Ergebnis Team 1

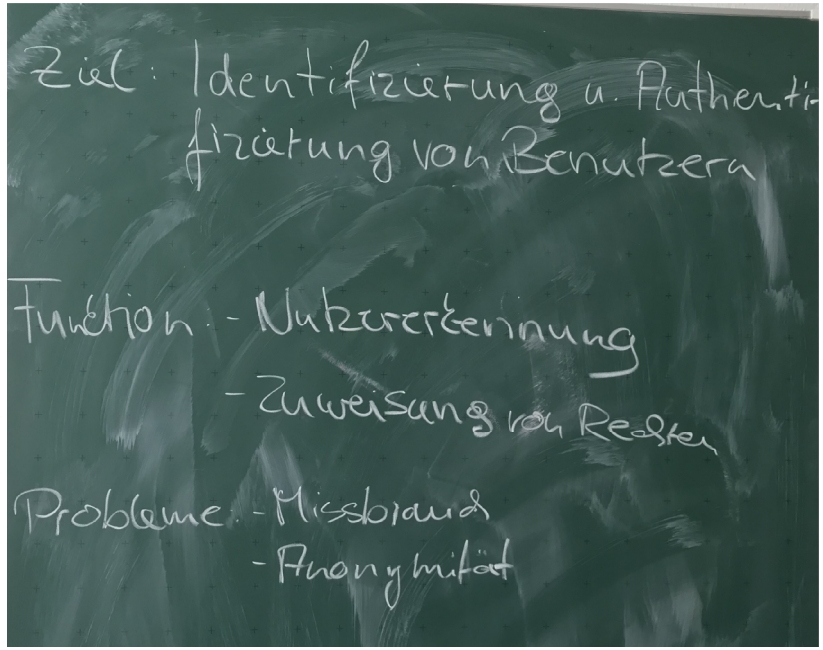
Bemerkungen:

HTTP Basic Authentication

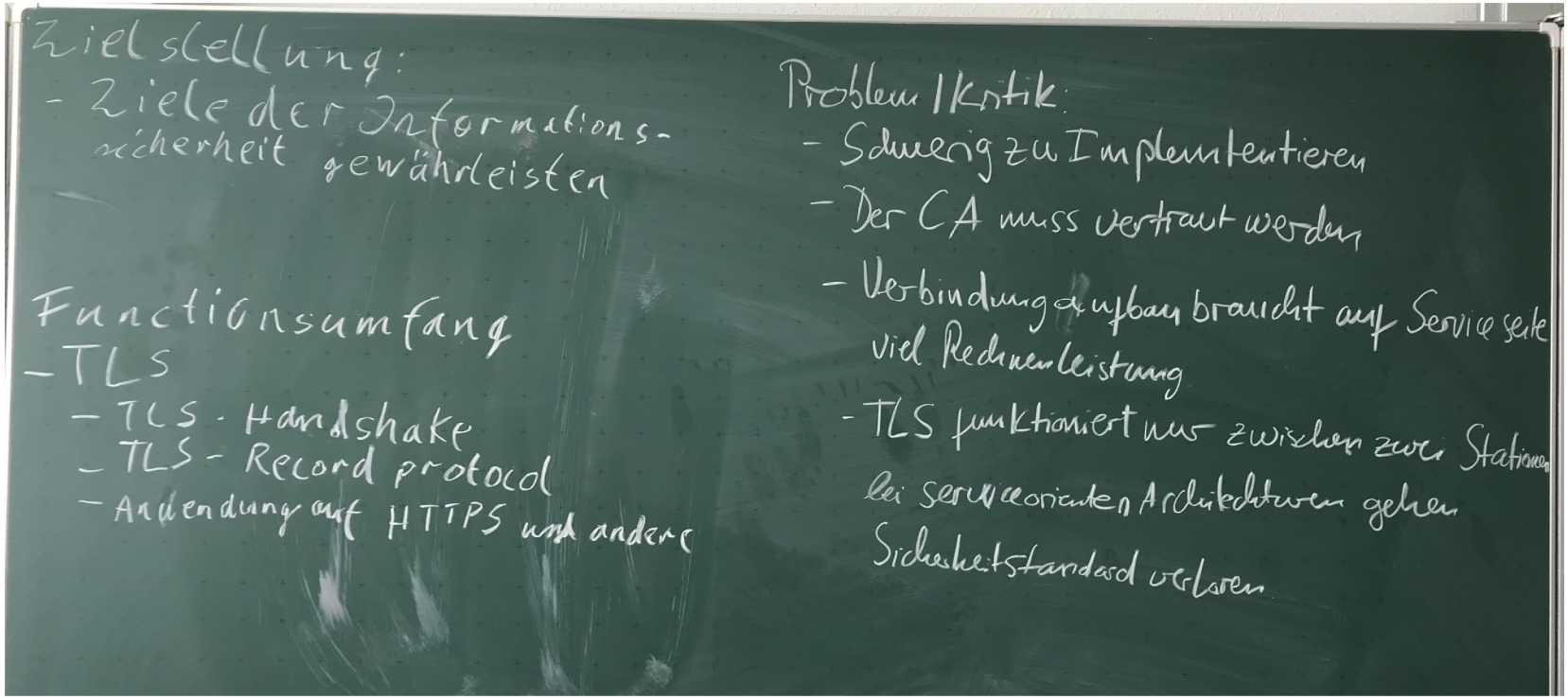
- Nutzername/Passwort
- Keine Verschlüsselung!
- typ. Kombination mit TLS (zwingend)

OAuth 2.0

- Protokoll Übertragung von Rechten
- Verschiedene Akteure (Ressourceserver, Ressourcenbesitzer, Client, Autorisierungserver)
- Client benötigt Token vom Autorisierungsserver



Ergebnis Team 2



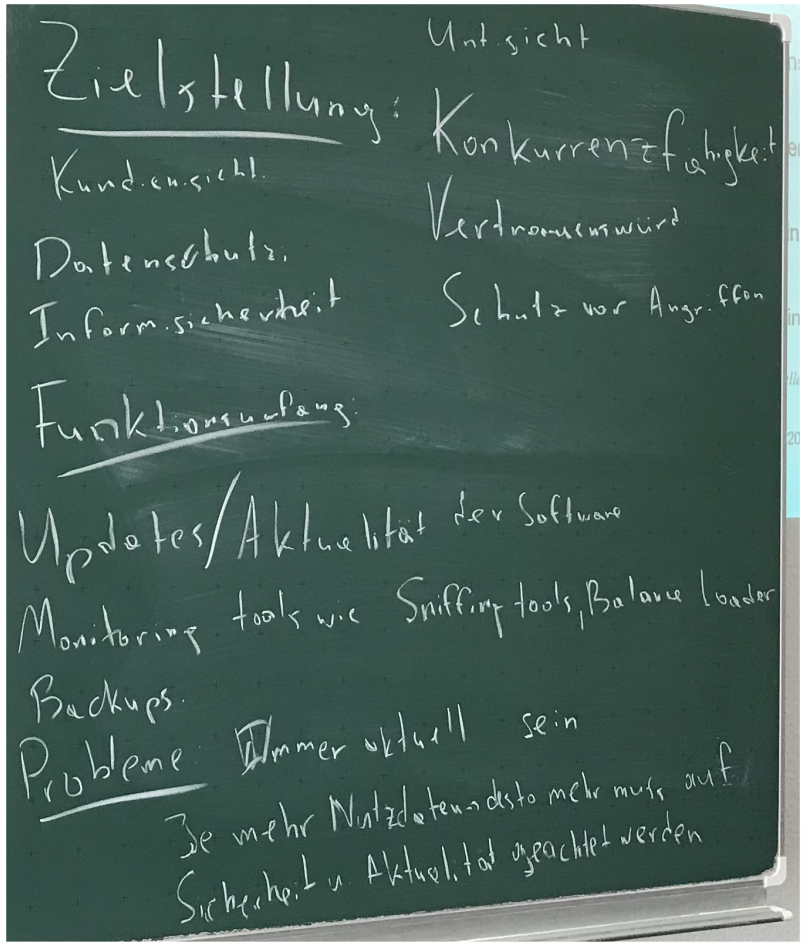
Bemerkungen:

- TLS Transport Layer Security
- CA - certificate authorities (z.B. Deutsche Telekom oder auch Unis)

Ergebnis Team 3

Bemerkungen:

- Aktualität von HW & SW gewährleisten
- Identifikation von Schwachstellen
- Kennen bekannter Sicherheitsprobleme
- Hochwertige Administration sichern
- Netzwerküberwachung mittels Sniffer und Einsatz analytischer Methoden (z.B. Big Data)



Ergebnis Team 4