Sicherheit

Nur eines ist sicher: **nichts ist sicher!** Folgende Regeln und Tipps helfen uns, sichere Applikationen und Angebote zu erstellen.

Beim Programmieren und Konfigurieren stelle ich mir folgende Fragen und verfolge diese Grundsätze:

Regeln:

- Ich kenne die aktuellen Bedrohungen gemäss der OWASP Top 10 und weiss, wie ich damit umgehen kann (Cheat-Sheet).
- Whitelisting ist besser als Blacklisting. Will heissen, ich schalte nur die Möglichkeiten und Funktionen auf, die effektiv benötigt werden.
- Ich kenne und nutze die Sicherheitsfeatures, die von der verwendeten Technologie angeboten werden.

Fragen:

- Habe ich keine Hintertür offen lassen?
- Habe ich meine Testaccounts gelöscht?
- Kann nachvollzogen werden, was auf den System passiert? Sind Logfiles vorhanden, kann darauf zugegriffen werden, sind sie geschützt, werden Benutzeraktionen protokolliert?

Best Practices:

Cookies

- Cookies sollen immer kurze Laufzeiten haben, respektive nicht länger gültig sein als die zu erwartende Lebensdauer von Sessionen. Ausnahme davon sind gewisse Tracking-Cookies
- Es werden keine vertraulichen Daten in Cookies gespeichert. Je weniger Daten, desto besser.
- Cookies sind mit den Attributen **httpOnly** und **secure** zu versehen.