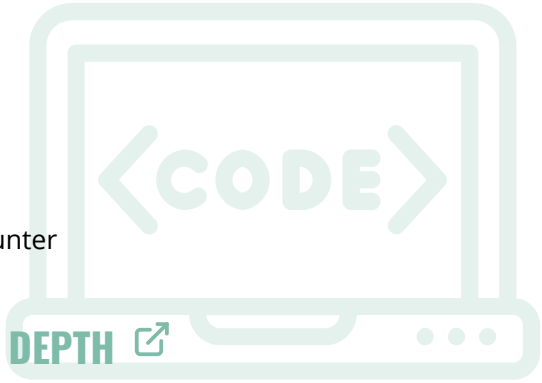
15 PRINZIPIEN FÜR SICHERE SOFTWARE

Mehr zu dem jeweiligen Prinzip erfahren Sie per Klick auf das Prinzip oder unter viadee.de/sicherheitsprinzipien



KISS

Keep It Simple, Stupid: Sicherheitsfunktionen robust und einfach implementieren.

POSITIVES SICHERHEITSMODELL

Der Grundgedanke ist: explizit Erlauben (White Listing / Allow List) statt explizit Verbieten (Black Listing / Block List).

BEHEBE DIE URSACHEN

Eine Root-Cause-Analyse führt zum Kern des Problems. Hier Korrekturen vorzunehmen führt zu langfristig korrekten und wartbaren Code.

MINIMIERE PRIVILEGIEN

Dem Least Privilege-Prinzip folgen: Nur erforderliche Berechtigungen. Wenn User:innen Aufgaben nicht mehr durchführen, Berechtigungen wieder entfernen.

VERMEIDE RISIKEN

Auf die Kernkompetenzen der Software konzentrieren – Mut zum Delegieren.

MINIMALPRINZIP

Definiere die Schnittstellen des Software-Systems so schlank wie möglich. Keine unnötigen Parameter, Technologien oder Daten anbieten.

SECURE BY DESIGN

Sicherheitsmaßnahmen in den gesamten Softwarelebenszyklus integrieren und bereits frühzeitig beim Entwurf sicherheitsrelevante Entscheidungen treffen.

VERTRAUE NIEMANDEN

Vertraue keinen anderen Systemen oder Akteuren (Zero Trust) und validiere externe Dateneingaben.

DEFENSE IN DEPTH

Mehrschichtige Security Controls treten Risiken entgegen: Fällt ein Control aus, sorgen andere Controls für Sicherheit.

KERCKHOFFS'SCHE PRINZIP

Bei Verschlüsselungsverfahren ist der Schlüssel nicht der Verschlüsselungs-algorithmus geheim zu halten. Keine Security by Obscurity!

KENNE DEINEN GEGNER

Eine Risikoanalyse hilft konkrete Gefahren-szenarien zu ermitteln, einzuschätzen und zu bewerten. Maßnahmen können dann effizient und effektiv geplant werden.

KONSISTENTE SICHERHEIT

Ein System ist nur so sicher, wie sein schwächstes Glied: Maßnahmen konsistent auslegen.

FAIL SECURE

Bei Fehlern geht das System nicht in einen sicherheitsgefährdenden Zustand über.

ARBEITE BENUTZERFREUNDLICH

Sicherheitsmechanismen so implementieren, dass sie Akzeptanz bei den Nutzenden schaffen und nicht umgegangen werden.

VERWENDE INDIREKTIONEN

Implementiere Indirektionen als Ergänzung zu dedizierten Zugriffskontrollen. Indirektionen mappen von einer extern bekannten Repräsentation von Daten in eine nur intern bekannte Repräsentation der Daten.