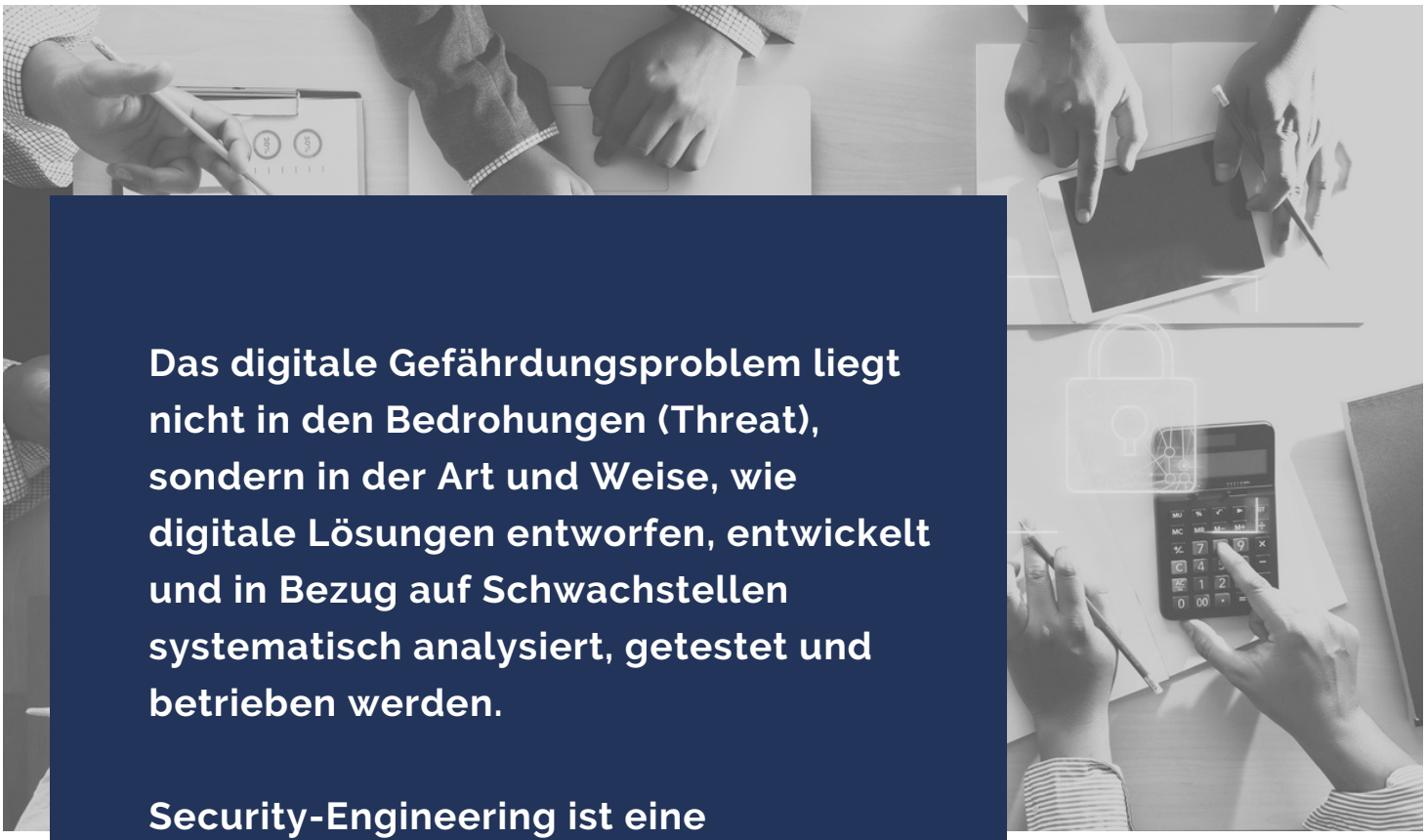
Trust K|B|B

Architekturbüro für intelligente IT-Sicherheit

Exposé | Security Engineering | 05.2022

SECURITY ENGINEERING



Das digitale Gefährdungsproblem liegt nicht in den Bedrohungen (Threat), sondern in der Art und Weise, wie digitale Lösungen entworfen, entwickelt und in Bezug auf Schwachstellen systematisch analysiert, getestet und betrieben werden.

Security-Engineering ist eine strukturierte Methodik, um digitale Systeme so zu gestalten, dass sie trotz äußerer Bedrohungen, ihre Funktionsweisen idealerweise ohne Schwachstellen bereitstellen können.

SECURITY MODELLING

Security-Engineering beginnt mit Methoden für ein Security-Modelling und einer begleitenden, modellgestützten Sicherheitsbewertung

Die Zusammenführung eines funktional ausgerichteten Architekturdesigns mit einer modellgestützten Gefährdungs-bewertung legt den Grundstein für das Design einer angemessenen Sicherheitsarchitektur (Security-by-Design).

Abgeleitete Sicherheitsfunktionen sind Ergebnis begründeter Entscheidungen unter Anwendung einer formalen Beschreibung von Sicherheits-problemen (Security Problem Definition).

Der Schutzbedarf identifizierter Assets leitet sich direkt aus einer Sicherheits-strategie ab.

Ihre konsequente technische Umsetzung fordert jedoch transformierende Instrumente und Regeln (Security- Policy-Enforcement) für eine wirksame Durchsetzung auf allen Architektur-Ebenen.

SECURITY MODELLING

Security by Design

Jede Entscheidung zur Entwicklung einer Sicherheitsarchitektur begründet sich auf dem Ergebnis einer strukturierten Gefährdungsbewertung.
Digitale Unternehmenswerte werden darüber transparent und bleiben auf allen Ebenen der Lösungsarchitektur im Fokus.

Security Problem Defintion

Die Formulierung eines Sicherheitsproblems als Modell setzt den Ausgangspunkt zur Entwicklung einer Sicherheitsarchitektur. Die Identifizierung von Sicherheitsproblemen orientiert sich an der Verteilung der zu schützenden Assets und erfordert eine strukturierte Methodik.

Security Policy Enforcement

Prozesse unterziehen sich einer Dynamik von regulativen Anforderungen. Das Architekturdesign muss daher strategische Schnittstellen für ein übergreifendes Policy-Management berücksichtigen. Policy-Beschreibungen formulieren Erwartungswerte und sind Ausgangspunkt für die adaptive Neuausrichtung regulierter Rahmenbedingungen.

Security Solution Definition

Die Entscheidung für die Anwendung eines Sicherheitsdesigns und die Anwendung von Sicherheitsfunktionen orientieren sich an den gestellten Sicherheitszielen. Security Modelling erlaubt eine zeitnahe Verknüpfung zwischen Sicherheitszielen und Elementen des Sicherheitsentwurfs zur Lösung der Sicherheitsprobleme.

BERATUNGSGEGENSTAND

Mit den Methoden für ein Security-Modelling wird ein funktional orientiertes Architekturdesign mit Ebenen einer Common-Criteria-orientierten und modellgestützten Gefährdungsbewertung übereinandergelegt (Security-by-Design).

Die Zusammenführung beider Perspektiven führt zu einem begründeten und angemessenen Entwurf einer IT-Sicherheitsarchitektur als Prozesslösung.

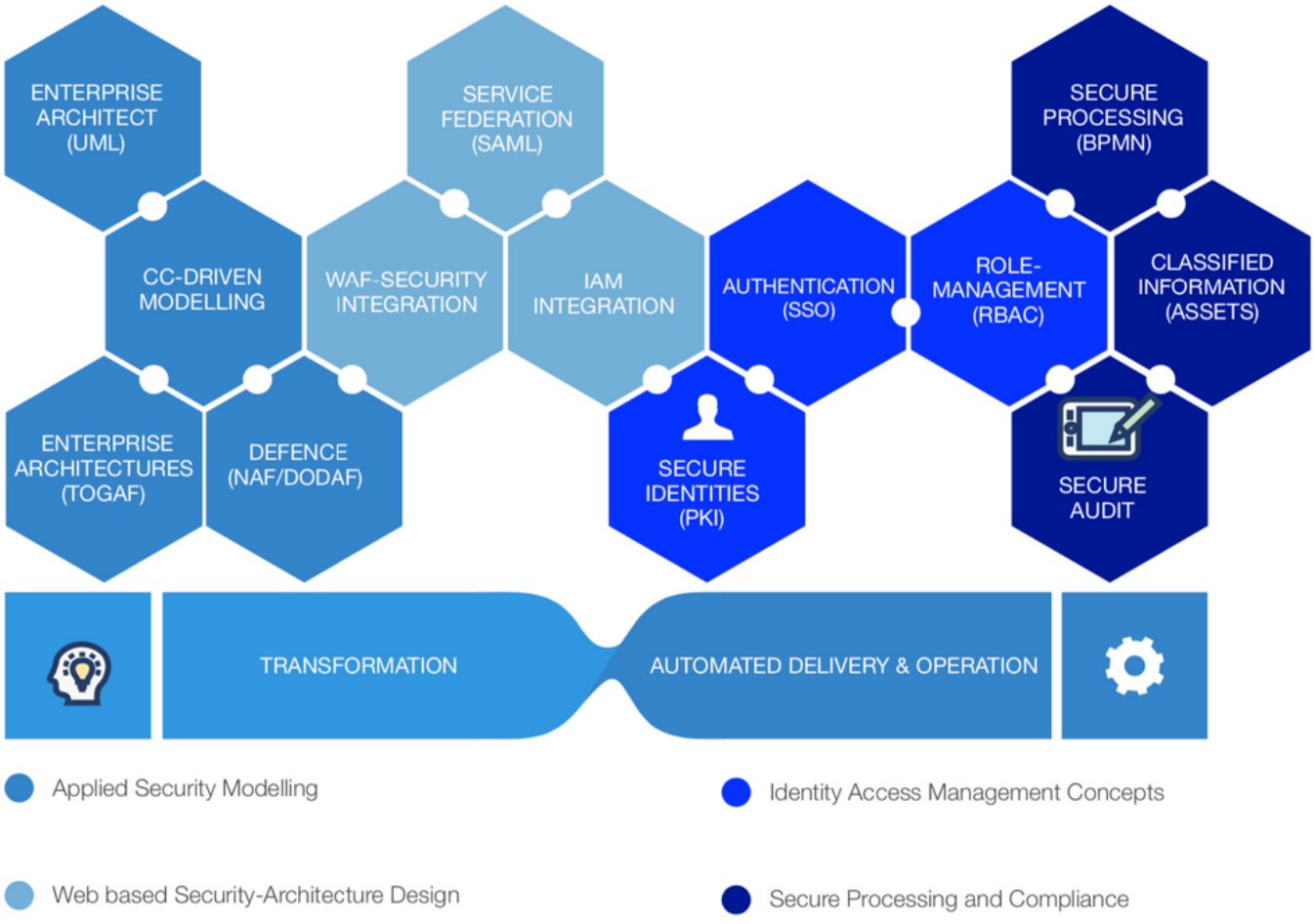
Der Entwurf von Sicherheitsarchitekturen bezieht alle Ebenen einer domänenspezifischen, digitalen Infrastruktur ein.

Die der Architekturentwicklung überlagerte Sicherheitsbetrachtung umfasst die Konzepte für Akteure (Identities), Netzwerke (VPNs, Router, Switche), Komponenten (ComputeNodes, Storages) und Strukturen (Organization, Roles) mit ihren Fachverfahren (Workflows) und Compliance-Anforderungen (Policies).

Leistungen der TrustKBB

Jedes Segment der Abbildung beschreibt einen Teilaspekt im ganzheitlichen Sicherheitsentwurf. Methodische Modellierungsansätze bilden den Ausgangspunkt einer automatisierbaren Transformation einer vorliegenden Sicherheitsstrategie in abgesicherte, reproduzierbare Sicherheitslösungen.

GANZHEITLICHER SICHERHEITSENTWURF



BERATUNGSGEGENSTAND

Leistungsbausteine auf einem Blick

- Modellgestützte Umsetzung eines ganzheitlichen Security Engineerings für IT-Architekturen
- Beratung für die Auswahl angemessener Sicherheitsfunktionen
- Modellbausteine zur Anwendung der CC-Prinzipien im Modell
- Vorgefertigte Modell-Funktionen, um notwendige Nachweise zur Sicherheitszulassung zur generieren
- Ableitung formaler Regelwerke für die konforme Umsetzung (Security-Policy-Enforcement)
- Unterstützungsleistungen für eine technische Transformation

Trust K|B|B

Friedrichstrasse 171
10117 Berlin
Telefon: +49 30 520045374
E-Mail: joerg.kebbedies@trustkbb.de