wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

PENETRATIONSTEST

T-SYSTEMS MULTIMEDIA SOLUTIONS

CERTIFIED SECURITY

T · · Systems ·

wegweisend digital

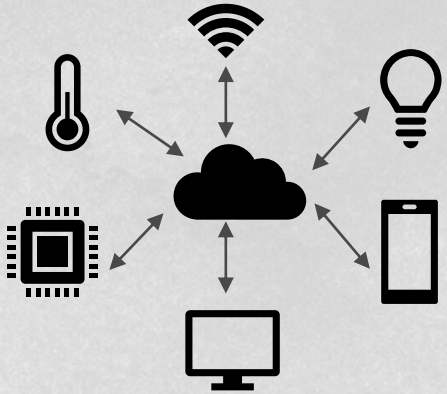
T-SYSTEMS MULTIMEDIA SOLUTIONS

MOTIVATION

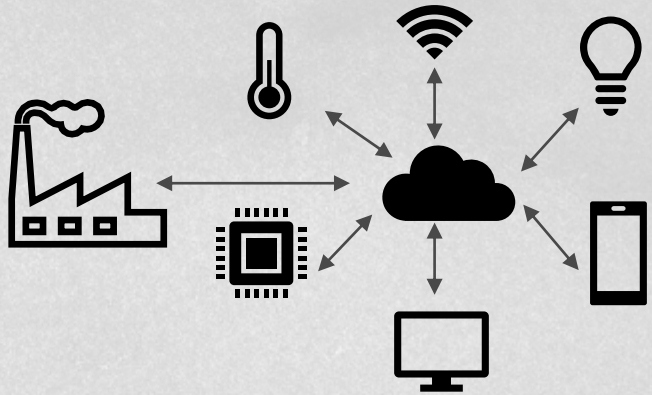
T · · Systems ·

ZUNEHMENDE VERNETZUNG
ERHÖHUNG DER KOMPLEXITÄT

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS



„intelligente“ Gegenstände mit „smarten“ Funktionen



Industrielle Ausprägung des IoT

T · · Systems ·

PENETRATIONSTEST

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

HERAUSFORDERUNG

- Aufspüren von Sicherheitslücken in Anwendungen oder IT-Infrastrukturen, bevor andere sie zu Ihrem Schaden ausnutzen können
- Bewertung des Sicherheitsniveaus von Anwendungen
- Beschreibung der identifizierten Schwachstellen
- Erstellung eines detaillierten Maßnahmenkataloges mit Empfehlungen

T · · Systems ·

wegweisend digital

T-SYSTEMS MULTIMEDIA SOLUTIONS

HACKING VS. PENETRATIONSTEST

T · · Systems ·

HACKING

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

- Skills?
- Motivation?

T · · Systems ·

GESETZESLAGE

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

Hackerparagraph §202c "Vorbereiten des Ausspähens und Abfangens von Daten"

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. **Passwörter oder sonstige Sicherungscodes**, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. **Computerprogramme**, deren Zweck die Begehung einer solchen Tat ist, **herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht**, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) § 149 Abs. 2 und 3 gilt entsprechend.

T · · Systems ·

PENETRATIONSTEST

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

- Rechtliche Absicherung
- Definierter Scope
- Definierter Testprozess
  - Abgestimmte Prüfpunkte
  - Reproduzierbare Ergebnisse

Zustimmung zur Durchführung einer Sicherheitsvorüberprüfung

Hiermit erteilt

→ → Kunde

→ ...

der → T-Systems Multimedia Solutions GmbH

→ Riesaer Straße 5

→ 01129 Dresden

die ausdrückliche Zustimmung zur Durchführung einer externen Sicherheitsüberprüfung von xxx im folgenden Zeitraum:

Zeitraum: → xxx

Die Durchführung der externen Sicherheitsvorüberprüfung erfolgt im Auftrag von Kunde.

Die Zustimmung umfasst die für eine Sicherheitsvorprüfung notwendigen Handlungen, Kunde ist über jede Handlung der Sicherheitsvorüberprüfung informiert und erteilt – insbesondere soweit durch die Handlungen der Sicherheitsvorüberprüfung Strafvorschriften bzw. sonstige einschlägige Vorschriften (insbesondere aufgrund des Telekommunikationsgesetzes – TKG – bzw. des Gesetzes über den Schutz von zugangskontrollierten Diensten und von Zugangskontrolldiensten – ZKDSG) berührt sein können – jedes erforderliches Einverständnis.

Die Haftung der T-Systems Multimedia Solutions GmbH für Schäden aufgrund der Sicherheitsvorüberprüfung wird ausgeschlossen, soweit nicht wegen Vorsatzes zwingend gehaftet wird. Verpflichtungen entstehen der T-Systems Multimedia Solutions GmbH aufgrund der Durchführung der Sicherheitsvorüberprüfung nicht.

→ ..... → ..... → .....

→ Ort → → Datum → → Unterschrift Kunde

T · · Systems ·

wegweisend digital

T-SYSTEMS MULTIMEDIA SOLUTIONS

SCOPE DEFINIEREN

T · · Systems ·

ANGREIFERPERSPEKTIVE

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

Beschreibt mögliche Angreifer und deren Zugriffsmöglichkeiten, Privilegien, Voraussetzungen

Gegen welche Art Angreifer soll das System geschützt werden?
→ **Perspektive, welche der Tester während des Tests einnimmt**

Beispiele:
Externer, privilegierter Angreifer (z.B. Käufer, Endnutzer)
Interner, niedrig privilegierter Angreifer (z.B. Mitarbeiter)
Interner, hoch privilegierter Angreifer (z.B. Administrator)

→ Interne Angreifer (Mitarbeiter) werden oft nicht betrachtet

T · · Systems ·

TESTABDECKUNG

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

Legt fest, wie viele und welche Komponenten getestet werden sollen
→ **Testobjekte, welche im Rahmen des Tests untersucht werden**

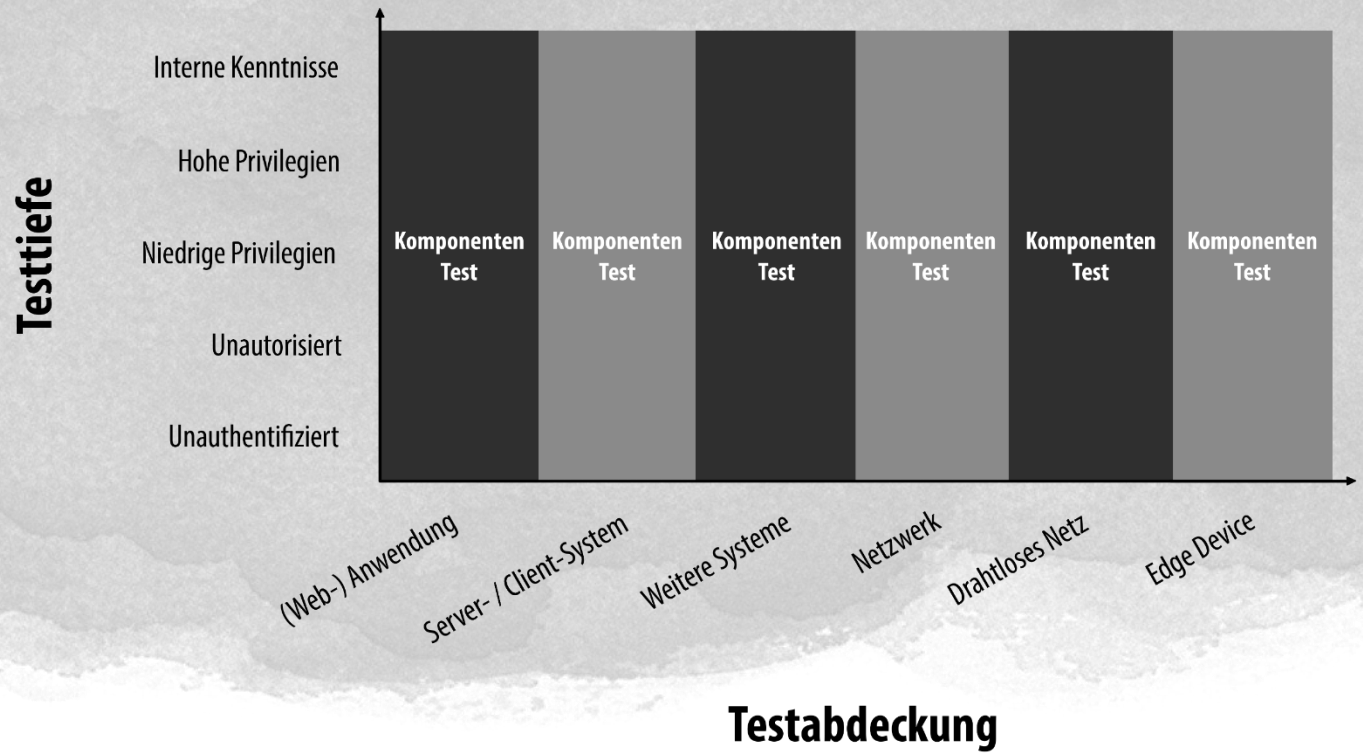
Beispiele:
Einzelne Komponenten (z.B. Webanwendungen, Server)
Einzelne Schnittstellen (z.B. APIs, Funkschnittstellen)
Ende-zu-Ende Test (vom Gerät über die API bis zur Webanwendung)

→ Zunehmende Vernetzung führt zu mehr Schnittstellen und zur vermehrten Öffnung dieser (Zugriff über das Internet)

T · · Systems ·

TESTABDECKUNG

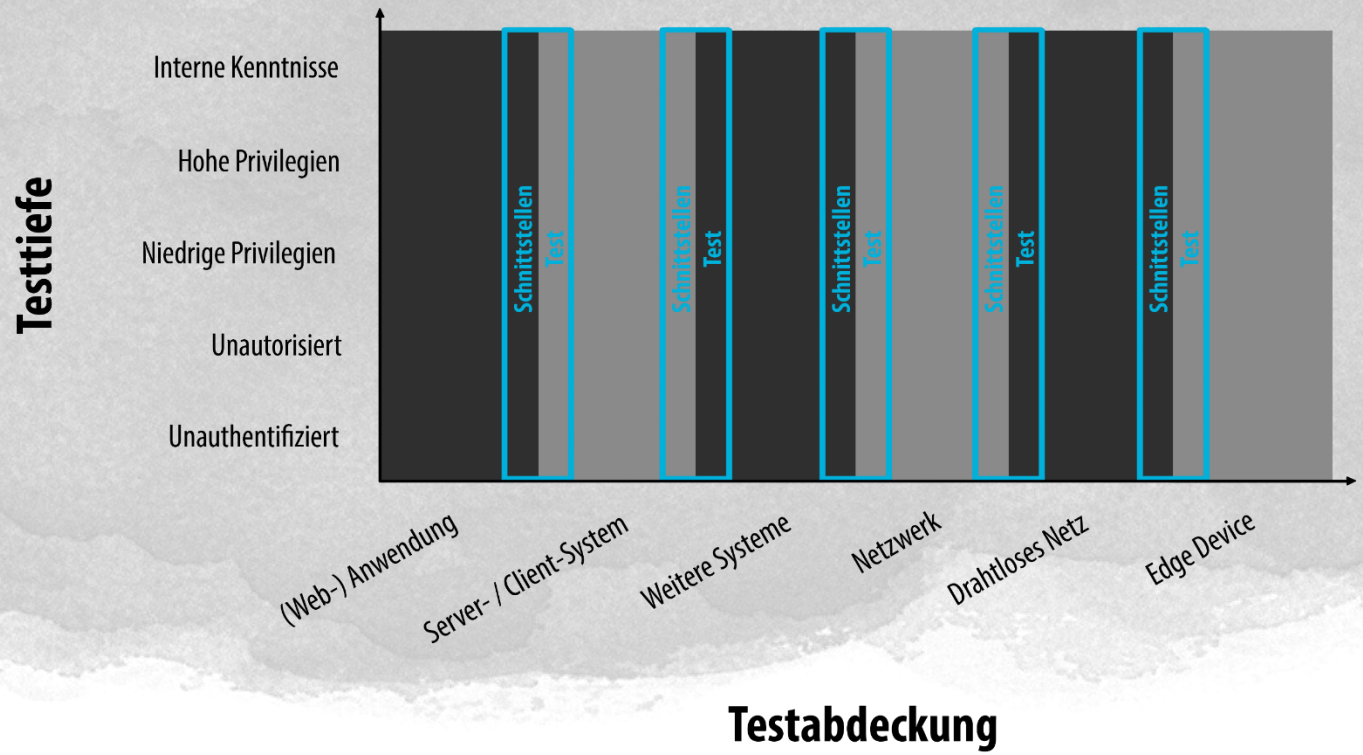
wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS



T · · Systems ·

TESTABDECKUNG

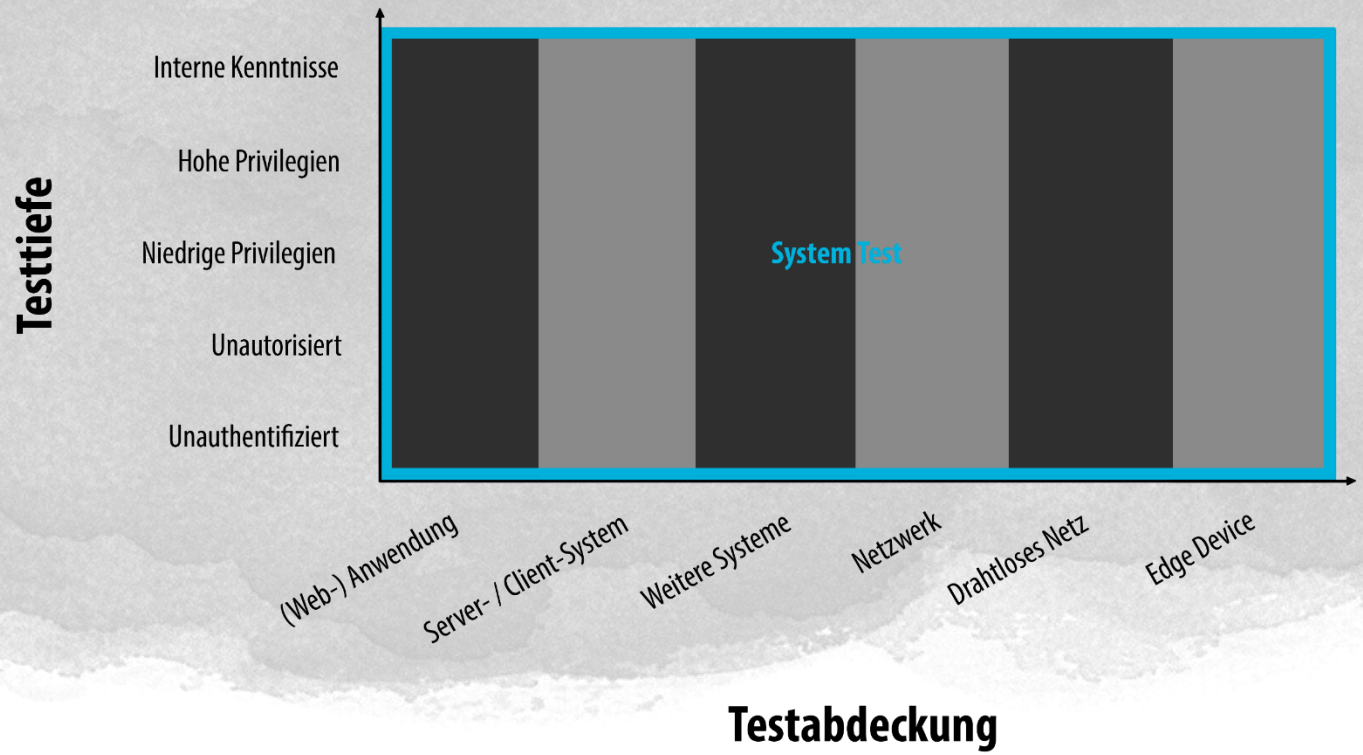
wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS



T · · Systems ·

TESTABDECKUNG

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS



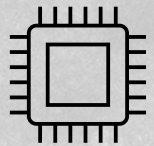
T · · Systems ·

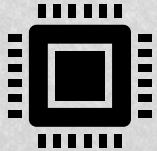
TESTABDECKUNG

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

Delta-Tests

Vergleich zwischen zwei verschiedenen Systemversionen





T · · Systems ·

TESTABDECKUNG

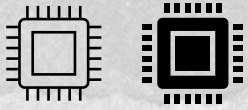
wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

Vergleich

- Teilsystemtest z.B. wichtig bei verschiedenen Zulieferern; Betrachtung aber nicht ganzheitlich
- Ende zu Ende betrachtet das System ganzheitlich; Aufwendiger und kostenintensiver
- Delta-Tests eignen sich bei weniger großen Updates

Teilsystem

Ende zu Ende



Delta-Tests

T · · Systems ·

TESTTIEFE

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

Legt fest, wie detailliert das Testobjekt betrachtet werden soll und welche Testfälle bzw. Testfallkategorien geprüft werden sollen

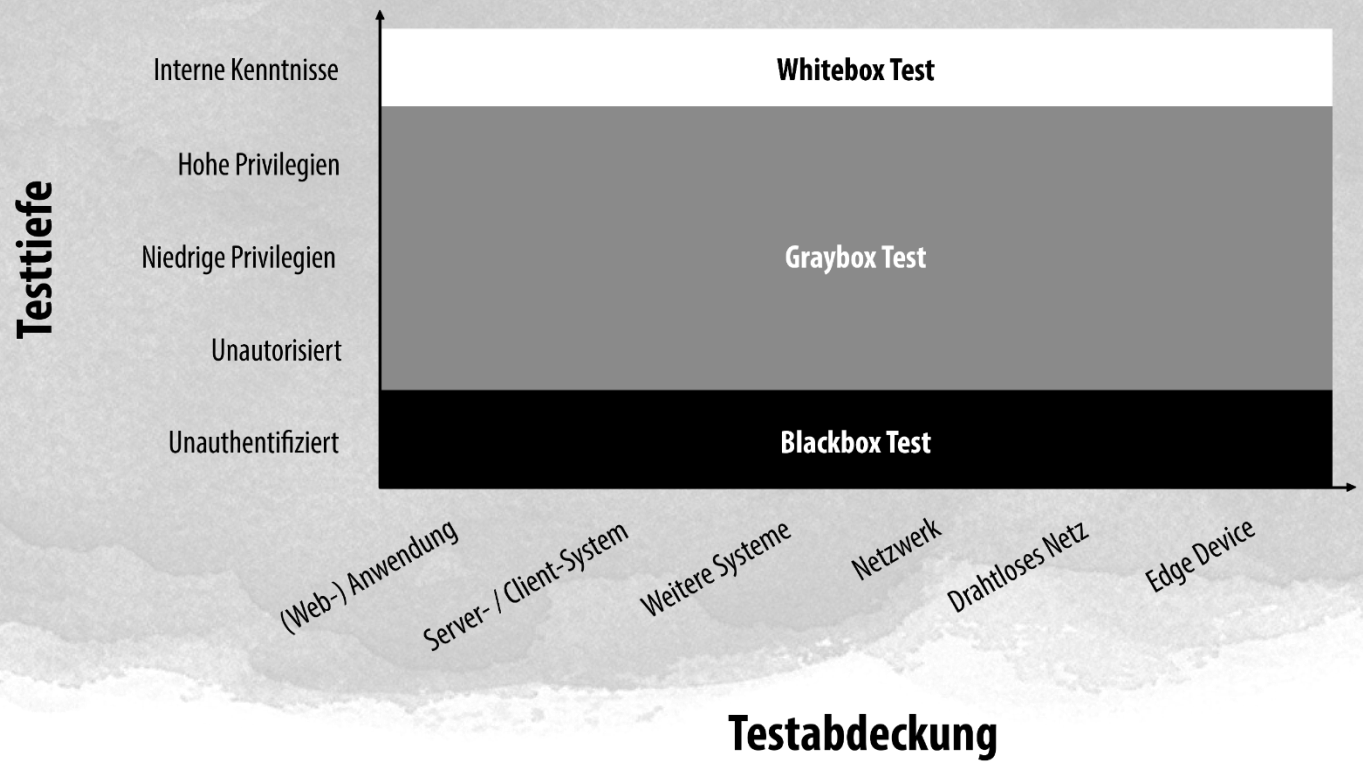
→ **Eingrenzung der Testfälle und der Einzelkomponenten, welche im Rahmen des Tests untersucht werden**

Beispiele:

- Blackbox (wenige bis gar keine Informationen über den inneren Aufbau des Systems vorhanden, unauthentifiziert, unautorisiert)
- Greybox (Mischform, z.B. wenige Informationen über den inneren Aufbau des Systems vorhanden, es liegen aber Anmeldedaten für Authentifizierung und Autorisierung vor)
- Whitebox (Details über den inneren Aufbau des Systems sind bekannt, der Tester hat Zugriff auf alle Einzelkomponenten)
- Explorativ oder time-boxed (der Tester entscheidet während des Tests, welche Einzelkomponenten in welcher Detailtiefe betrachtet werden)

TESTTIEFE

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS



T · · Systems ·

TESTTIEFE

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

Blackbox

- realitätsnah, vergleichsweise wenig Aufwand
- Probleme können übersehen werden
- relativ geringe Testabdeckung und hohes Risiko, dass tieferliegende Schwachstellen nicht entdeckt werden

Whitebox

- Besserer Soll-Ist Vergleich
- Aufgrund der Dokumentenlage können schon Probleme erkannt werden
- Aufgrund hoher Abdeckung meist auch höhere Kosten

T · · Systems ·

TESTTIEFE

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

Greybox

- Stellt eine Mischform aus Black- und Whitebox-Test dar
- Entsprechend geringere Kosten als bei Whitebox
- Nicht vollumfänglich wie Whitebox

Explorativ

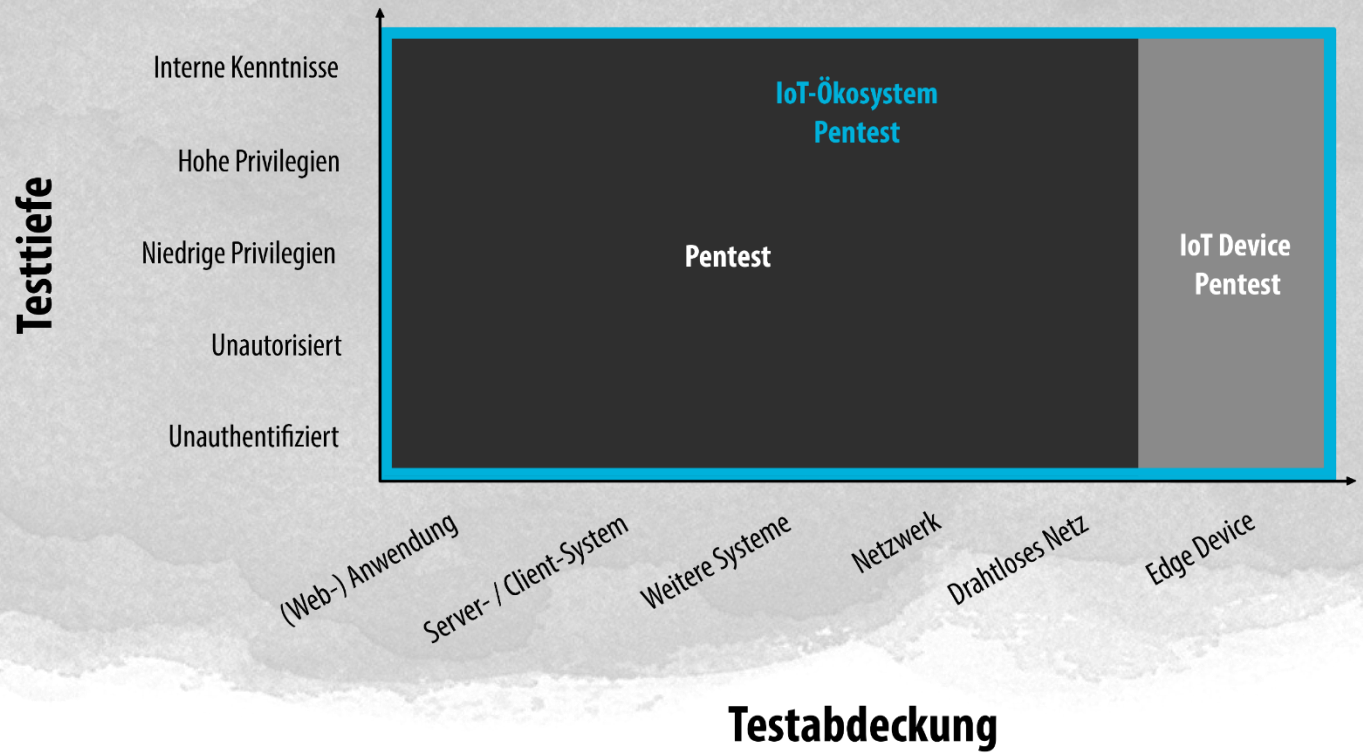
- Fokussiert auf das Wesentliche
- Meist festgelegter Zeitrahmen
- Besonders geeignet bei großen Systemen

T · · Systems ·

TESTSCHWERPUNKTE

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

Testschwerpunkte = Aspekte und Prüfpunkte, die während des Tests betrachtet werden



T · · Systems ·

TESTARTEN: SCHWACHSTELLENSCAN

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

- Mittels eines **Portscanners** und eines **Schwachstellenscanners** werden die **definierten IP-Adressen bzw. Anwendungen gescannt, um bekannte Schwachstellen zu identifizieren**.
- Mit Hilfe der vom Scanner genutzten Profile und Pattern können bekannte Schwachstellen in den Systemen und Webanwendungen erkannt und dokumentiert werden.
- Der **halbautomatisierte Schwachstellenscan** gibt einen **guten Überblick über das Sicherheitsniveau**, da typische Schwachstellen schnell identifiziert werden können.

T · · Systems ·

TESTARTEN: PENETRATIONSTEST

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

- Ein Penetrationstest bedeutet den **zielgerichteten Versuch, mit den Mitteln eines Angreifers innerhalb einer gegebenen Zeitspanne Lücken in der Sicherheit einer Anwendung oder eines Systems aufzudecken**.
- Aufgrund des **realitätsnahen Ansatzes** entsprechen die Methoden weitestgehend denen von potenziellen Angreifern.
- Das Vorgehensmodell baut auf dem Durchführungskonzept für Penetrationstests des Bundesamtes für Sicherheit in der Informationstechnik auf
- Durch die kontrollierte Durchführung von Angriffen im Rahmen eines Penetrationstests werden Schwachstellen der Systeme aufgedeckt. So wird von vornherein das Risiko minimiert, dass später ein echter Angriff Erfolg haben kann.

T · · Systems ·

TESTARTEN: SOURCE CODE ANALYSE

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

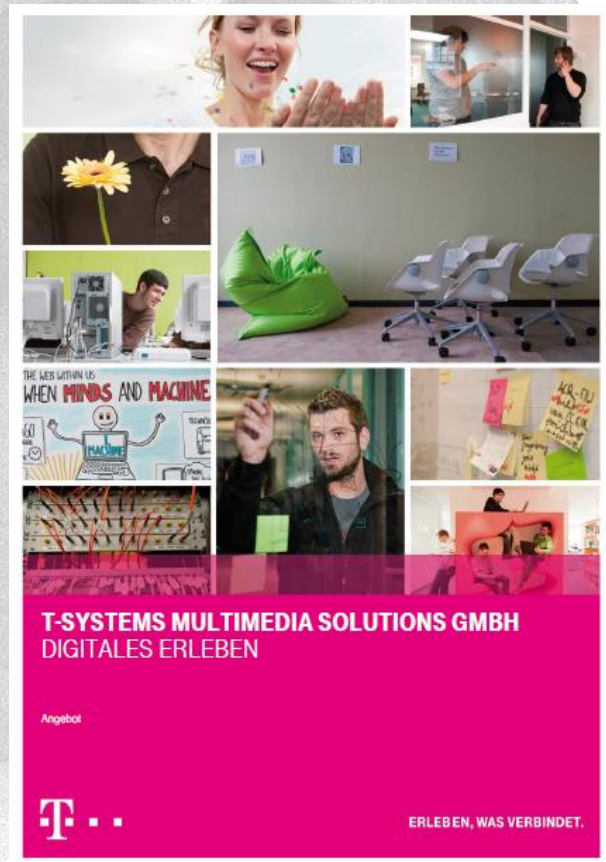
- Security Source Code Analyse bezeichnet die **Untersuchung von Quelltexten** und dient der Verbesserung und **Qualitätssicherung** von Applikationen.
- Im Rahmen der **automatischen Analyse** wird der Programmcode mit Hilfe sogenannter Metriken hinsichtlich besonderer Auffälligkeiten oder Verstößen gegen geltende Programmierrichtlinien mittels eines entsprechenden Werkzeugs geprüft. Bedingung für die Durchführung der Quellcodeanalyse ist die Lieferung des kompilierbaren, vollständigen Quellcodes, inklusive aller verwendeten Frameworks und Bibliotheken sowie Konfigurationsdateien.

T · · Systems ·

DAS ANGEBOT

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

- Testart und Testschwerpunkte (Scan, Penetrationstest,...)
- Auswahl der Testsysteme
- Whitebox oder Blackboxtest,
- Innen- oder Außenperspektive
- Sichtbarkeit (verdeckt oder offen)
- Testtiefe
- Planung der Testdurchführung
    - Testzeitraum
    - Testzugänge, Testaccounts
    - Mitwirkung des Kunden



T · · Systems ·

wegweisend digital

T-SYSTEMS MULTIMEDIA SOLUTIONS

TESTVORGEHEN

T · · Systems ·

VORGEHENSMODELL

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

5-Phasen Modell des Bundesamtes für Sicherheit in der Informationstechnik (BSI):

1. Vorbereitung
2. Informationsbeschaffung und –auswertung
3. Bewertung der Informationen / Risikoanalyse
4. Aktive Eindringversuche
5. Abschlussanalyse

T · · Systems ·

VORGEHEN PENTEST
PHASE 1

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

T · · Systems ·

VORGEHEN PENTEST
PHASE 2

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

T · · Systems ·

VORGEHEN PENTEST
PHASE 3

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

T · · Systems ·

VORGEHEN PENTEST
PHASE 4

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

T · · Systems ·

VORGEHEN PENTEST
PHASE 5

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

T · · Systems ·

TESTWERKZEUGE

Je nach zu untersuchemden Testobjekt kann Spezial-Soft- / Hardware benötigt werden

Kali Linux
Web: BurpSuite (BURP), Swagger
Infra: nmap, WireShark, Metasploit, John the Ripper
....

→ Eigenes Modul in dieser Vorlesungsreihe.

BEWERTUNG VON FINDINGS

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

Bewertung: nach CVSS 3.0 (Base Score): https://www.first.org/cvss/calculator/3.0

Attack Vector	Network	Adjacent	Local	Physical
Attack Complexity	Low	High		
Privileges Required	None	Low	High	
User Interaction	None	Required		
Scope	Unchanged	Changed		
Confidentiality	None	Low	High	
Integrity	None	Low	High	
Availability	None	Low	High	

→ Score: 7,6 (High)

T · · Systems ·

TESTBERICHT PENETRATIONSTEST

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

TESTBERICHT T-SYSTEMS MULTIMEDIA SOLUTIONS
PENETRATIONSTEST

Projektnummer:	
Version:	1.5
Stand:	04.12.2013
Dateiname:	Testbericht_Penetrationstest_V1.5.docx
Für:	Auftraggeber
Testgrundlage:	(in Anlehnung an) DIN ISO / IEC 25051 DIN ISO / IEC 25010
Testzeitraum:	07.10.2013 bis 22.10.2013

T · · Systems ·

wegweisend digital

T-SYSTEMS MULTIMEDIA SOLUTIONS

T-SYSTEMS MMS

T · · Systems ·

BA CERTIFIED QUALITY – DAS TEST AND INTEGRATION CENTER

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

DAkkS
Deutsche Akkreditierungsstelle
D-PL-12012-01-01

DAS TEST AND INTEGRATION CENTER

der T-Systems Multimedia Solutions GmbH ist ein von der Deutschen Akkreditierungsstelle (DAkkS) akkreditiertes Software-Prüflabor. Als BSI zertifizierter IT-Sicherheitsdienstleister mit 300+ Quality-Engineers und Security-Spezialisten sorgen wir für die Digitale Zuverlässigkeit von Geschäftsprozessen, Anwendungen und IT-Systemen unserer Kunden.

T · · Systems ·

CERTIFIED SECURITY: UNSER TEAM

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

Zertifiziertes Testlabor + 60 Experten im Bereich Penetrationstest und IT – Forensik

- Berater,
- Forensiker,
- Penetrationstester,
- Projektmanager,
- Auditoren

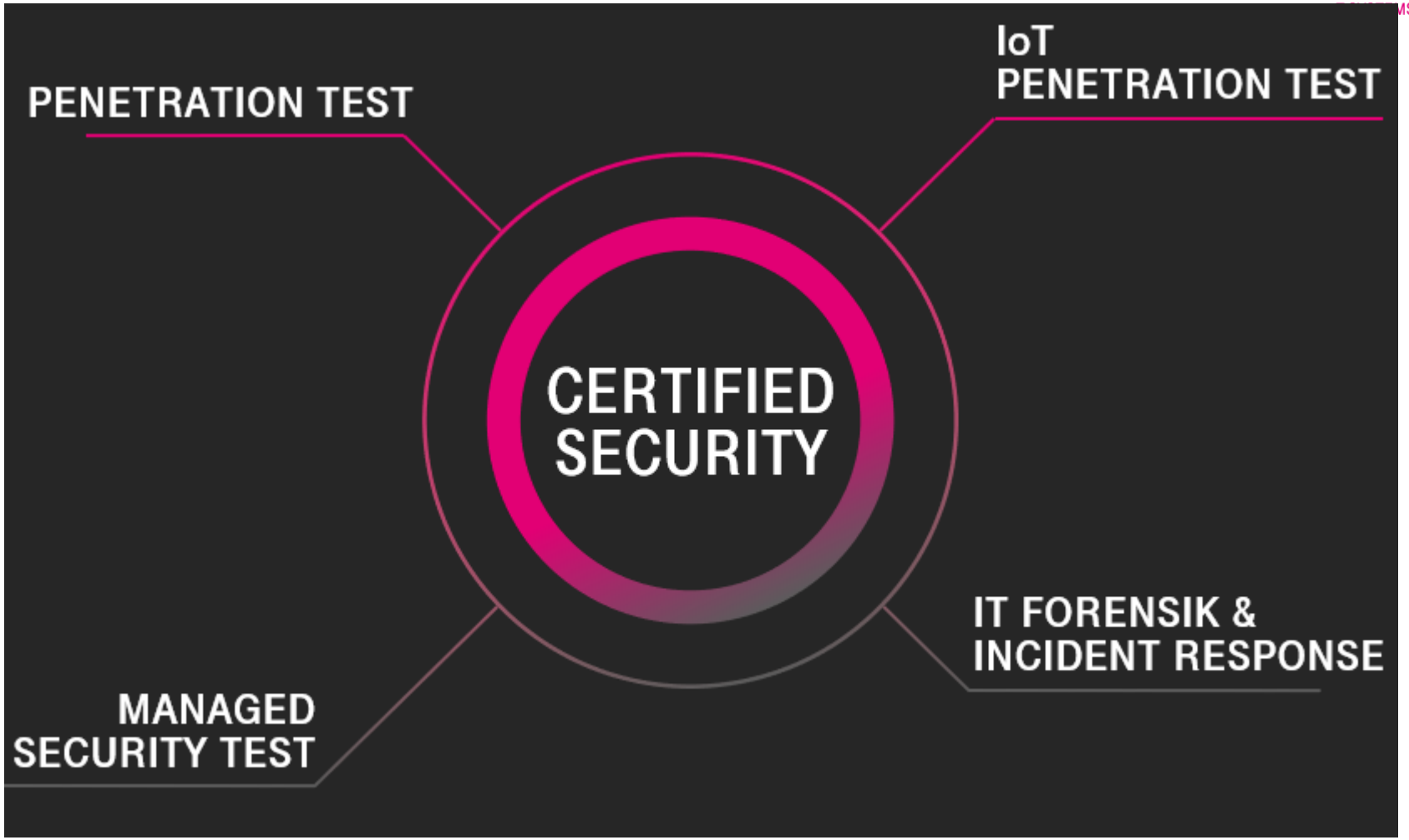
anerkannte Zertifizierungen: z.B. als

- Certified Ethical Hacker (CEH)
- ISTQB Certified Tester, Test Manager
- Certified Scada Security Architect (CSSA)
- Practical IoT Hacking Basic Edition
- Low-Level Hardware Reversing
- Side-Channel Attacks 101
- Practical Car Hacking
- Offensive Security Certified Professional (OSCP)
- Offensive Security Certified Expert (OSCE)
- GIAC Mobile Device Security Analyst
- Certified Security Analyst (ECSA)

T · · Systems ·

CERTIFIED SECURITY

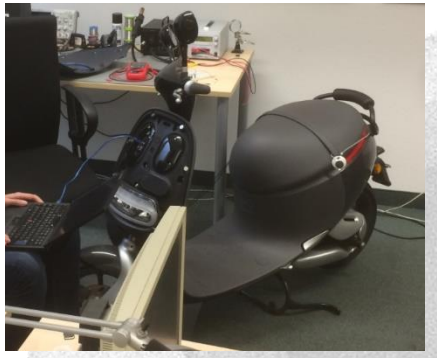
wegweisend digital
MULTIMEDIA SOLUTIONS

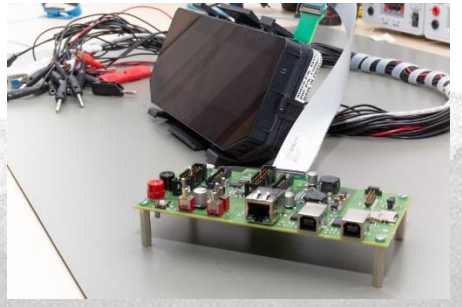


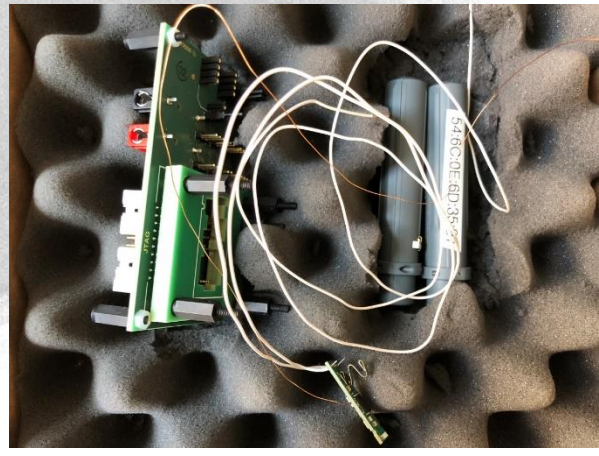
T · · Systems ·

CERTIFIED SECURITY

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS







T · · Systems ·

KONTAKT

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

DR. ANTJE WINKLER
T-Systems Multimedia Solutions GmbH

Riesaer Straße 5
D-01129 Dresden

Telefon: +49 351 2820 – 2093

E-Mail: antje.winkler@t-systems.com
Internet: www.t-systems-mms.com

T · · Systems ·