wegweisend digital

T-SYSTEMS MULTIMEDIA SOLUTIONS

PENETRATIONSTEST

T-SYSTEMS MULTIMEDIA SOLUTIONS

INFRASTRUCTURE AND APPLICATION SECURITY

T · · Systems ·

wegweisend digital

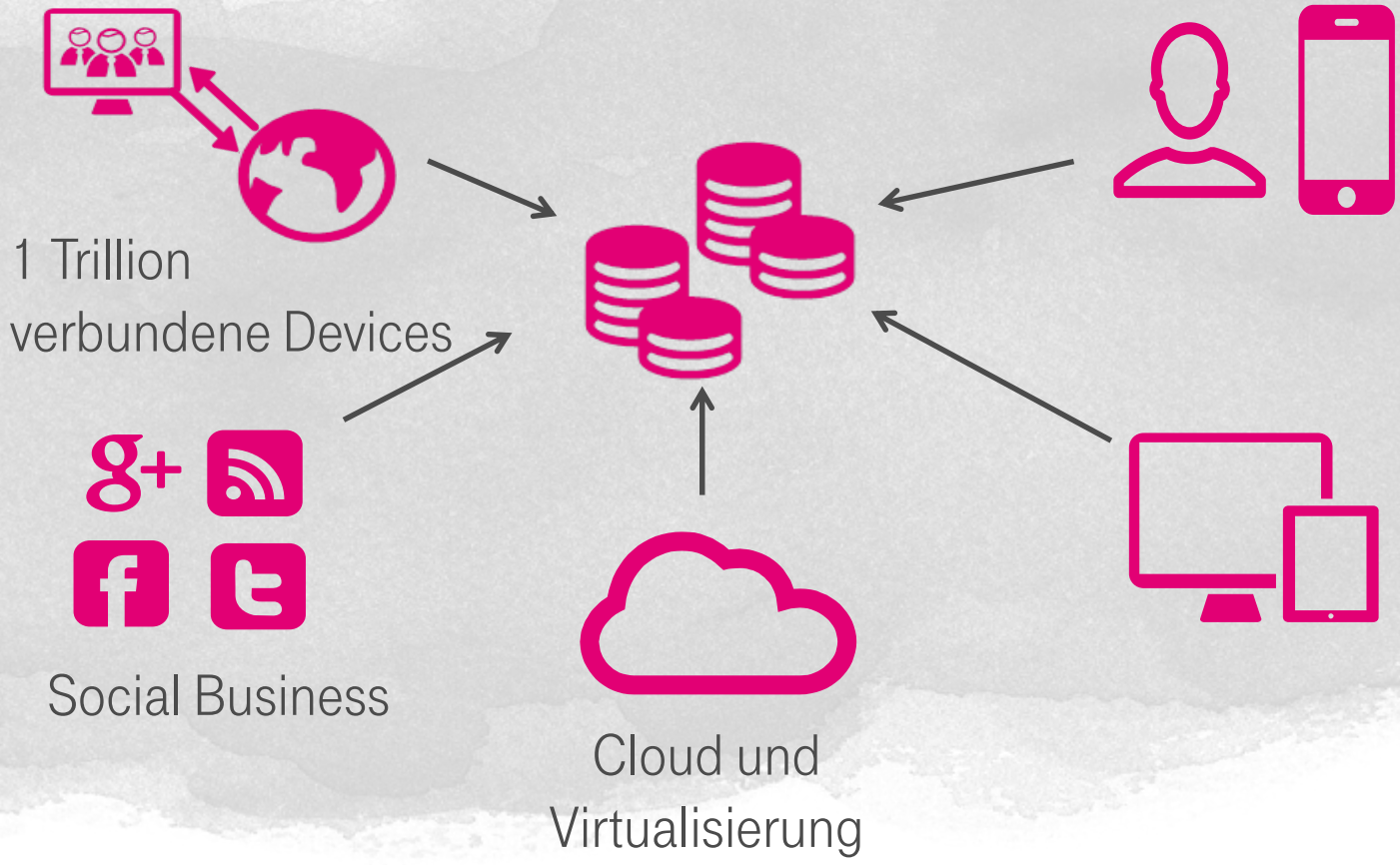
T-SYSTEMS MULTIMEDIA SOLUTIONS

MOTIVATION

T · · Systems ·

NEUES NUTZUNGSVERHALTEN
ERHÖHUNG DER KOMPLEXITÄT

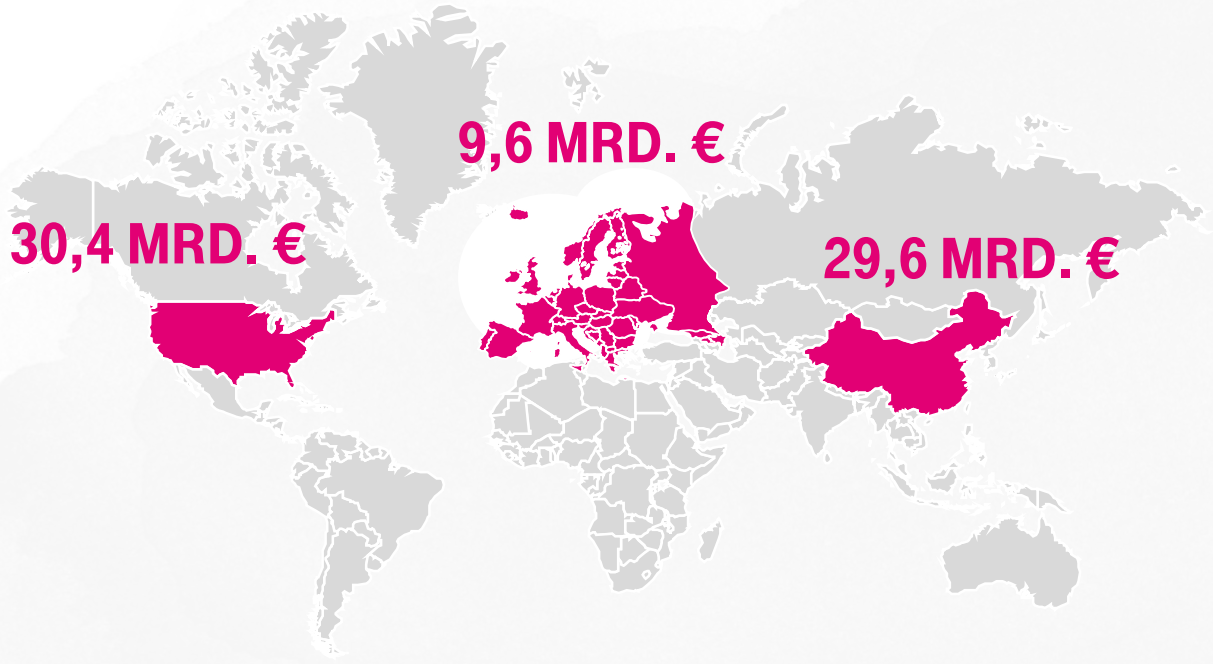
wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS



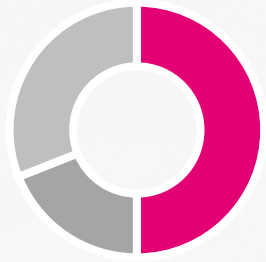
T · · Systems ·

SCHADENSPOTENTIAL
STETIG WACHSEND!

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS



Jährlicher Schaden durch Cybercrime (Norton)



Angriffe auf Unternehmen
(Symantec)

- >2.500 Mitarbeiter
- 251 - 2.500 Mitarbeiter
- 1 bis 250 Mitarbeiter

378
Millionen
Opfer pro Jahr
(Norton)

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

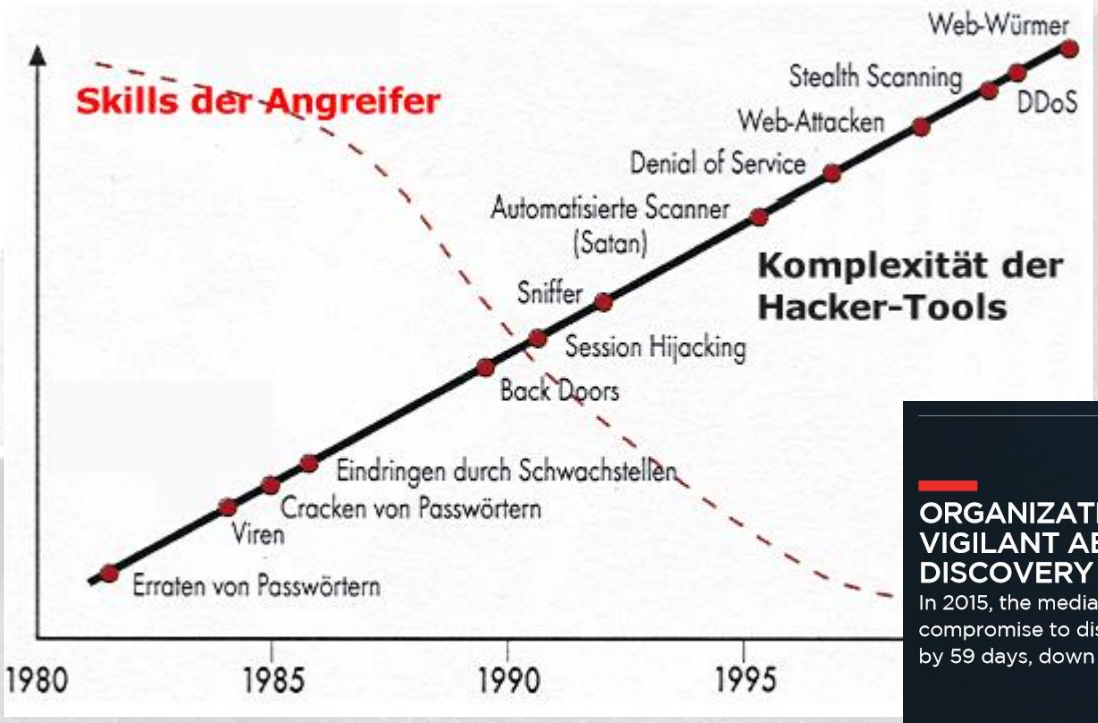
wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

- Skills?
- Motivation?

T · · Systems ·

HACKING

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS



ORGANIZATIONS MORE VIGILANT ABOUT DISCOVERY

In 2015, the median time from compromise to discovery was cut by 59 days, down from 205 days.

TIME FROM COMPROMISE TO DISCOVERY		
MEDIAN	EXTERNAL NOTIFICATION	INTERNAL DISCOVERY
146 DAYS	320 DAYS	56 DAYS

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
- Testprozess
  - Definierte 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

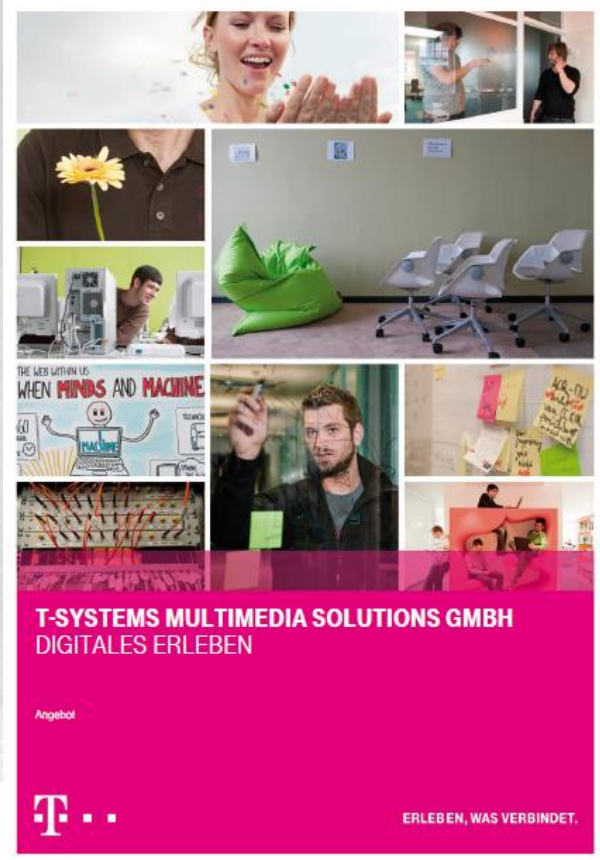
Die Durchführung der externen Sicherheitsvorüberprüfung erfolgt im Auftrag von Kunde.

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

DAS ANGEBOT - SCOPE DEFINIEREN

T · · Systems ·

ABSTIMMUNG MIT DEM KUNDEN

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 (passiv, agressiv)
- Planung der Testdurchführung
    - Testzeitraum
    - Testzugänge, Testaccounts
    - Mitwirkung des Kunden

T · · Systems ·

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 ·

BASIS SECURITY CHECK

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

Im Rahmen des Basis Security Check werden die Webanwendungen/die Infrastruktur aus der Position eines potentiellen Angreifers auf vorhandene Schwachstellen überprüft. Damit kann eine erste Einschätzung des Sicherheitsniveaus gegeben werden.

Ergebnisse:

- **Erste Analyse des Sicherheitsniveaus** einer Anwendung
- Auffinden einer Vielzahl einfach auszunutzender Sicherheitslücken
- **Dokumentation und Beschreibung** der gefundenen Sicherheitslücken sowie der möglichen Angriffsszenarien
- **Aufzeigen weiterer Testmöglichkeiten** und **Empfehlung von Maßnahmen** zum Schließen der Sicherheitslücken

T · · Systems ·

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 ·

TESTSCHWERPUNKTE

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

Systemkomponente	Testschwerpunkte
Webserver	- Überprüfung der Konfiguration - Untersuchung des Patchlevels - Untersuchung auf unsichere Beispieldateien und -skripte - Überprüfung der SSL-Konfiguration - Test auf frei zugängliche Verzeichnisse - Prüfung der erlaubten Webserver-Methoden

T · · Systems ·

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 ·

wegweisend digital

T-SYSTEMS MULTIMEDIA SOLUTIONS

DER TESTPROZESS

T · · Systems ·

VORGEHEN PENETRATIONSTEST
PHASE 1

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

T · · Systems ·

VORGEHEN PENTEST
PHASE 2

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

T · · Systems ·

TESTMODULE

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

Die Module, aus denen der Test laut der Anforderungen des Prüfverfahrens aufgebaut sein soll, sind jeweils durch einen eindeutigen *Namen* gekennzeichnet, dem ein „I“ (Modul zur Informationsbeschaffung) oder „E“ (Modul für aktive Eindringversuche) und die Nummer des Moduls vorangestellt wird:

- Beschreibung
- Ziel
- Voraussetzungen
- Hilfsmittel
- Aufgaben
- Risiken

T · · Systems ·

TESTMODULE

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

E 7. SQL-Injektion	
Beschreibung	
Wenn die Webanwendung mit einer SQL-Datenbank kommuniziert und bei der Kommunikation Parameter übergeben werden, die vom Client stammen, besteht die Gefahr von SQL-Injektion. Dabei werden vom Angreifer SQL-Fragmente an den Webserver geschickt, die dieser bei unzureichender Prüfung an den Datenbankserver weiterreicht.	
Ziel	
Ausführung von SQL-Code auf dem Server	
Voraussetzungen	Verwendung einer SQL-Datenbank
Hilfsmittel	Schwachstellenscanner
Erwartete Ergebnisse	
Liste mit Lücken, durch die SQL eingeschleust werden kann Informationen über den Aufbau der Datenbank (Feldnamen, Tabellennamen usw.)	
Aufgaben	Aufwand
SQL-Ausdrücke als Parameter an den Server schicken	hoch
Risiken	
Veränderung oder Zerstörung des Datenbestands.	

T · · Systems ·

VORGEHEN PENETRATIONSTEST
PHASE 3

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

T · · Systems ·

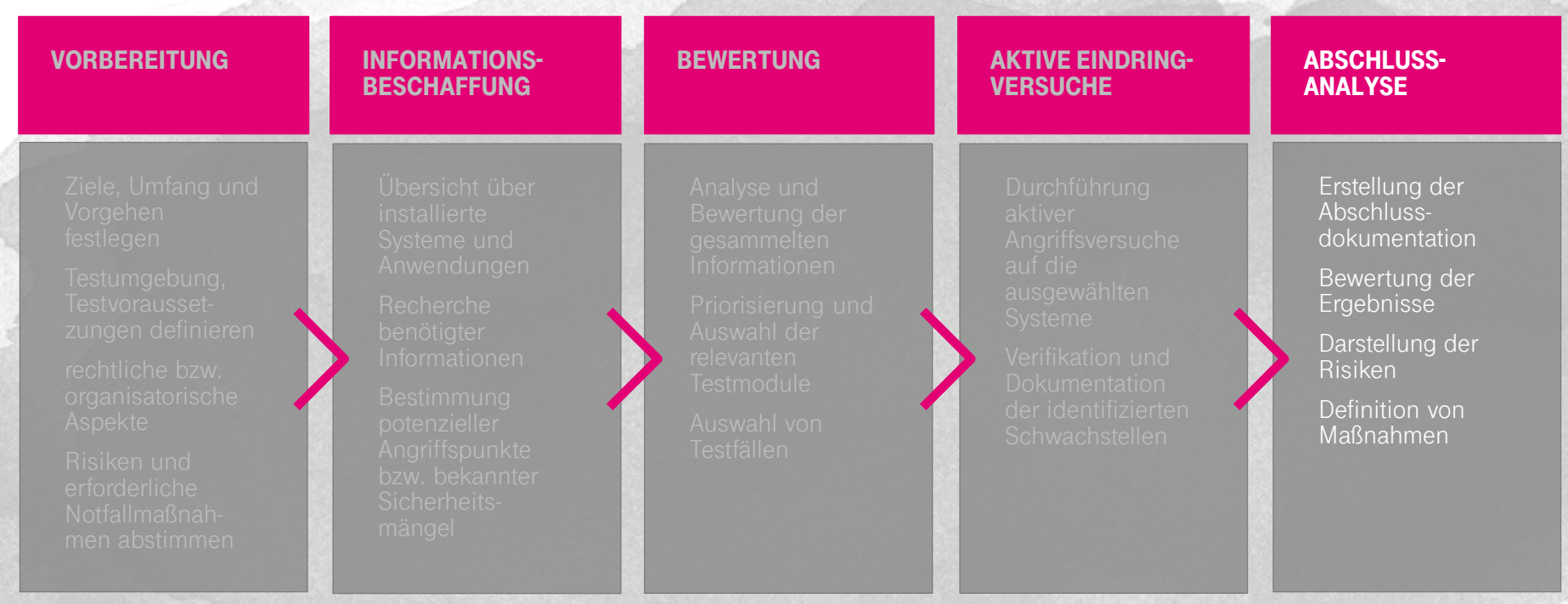
VORGEHEN PENETRATIONSTEST
PHASE 4

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

T · · Systems ·

VORGEHEN PENETRATIONSTEST
PHASE 5

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS



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 ·

TEST AND INTEGRATION CENTER

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

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

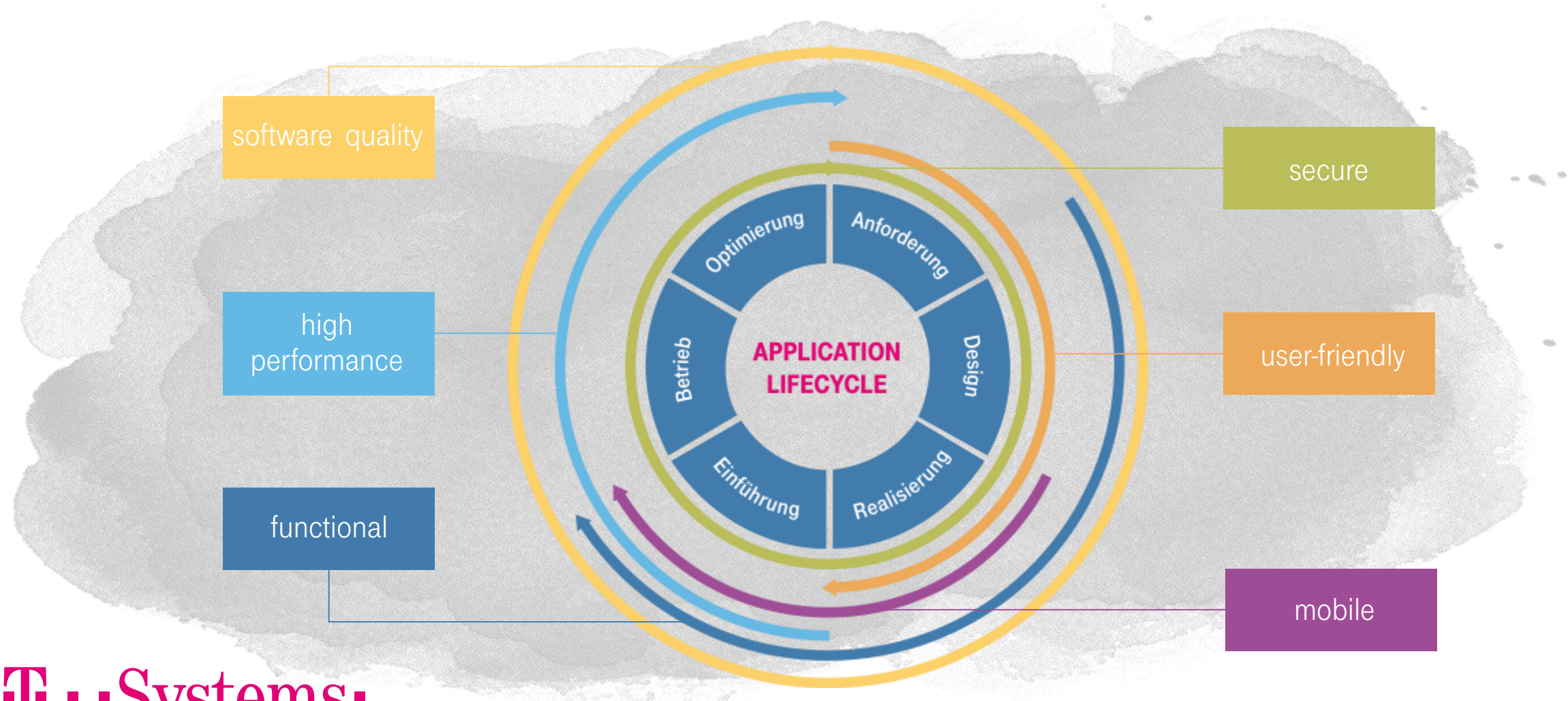
DAS TEST AND INTEGRATION CENTER von T-Systems Multimedia Solutions ist das einzige Softwareprüflabor der Internet- und Multimediabranche in Deutschland, das von der Deutschen Akkreditierungsstelle (DAkkS) anerkannt ist.

Mit über 175 ISTQB-zertifizierten Testexperten und 70 Spezialisten für IT-Security und Datenschutz prüfen wir die Qualität und Sicherheit von Web-Applikationen.

T · · Systems ·

TEST AND INTEGRATION CENTER

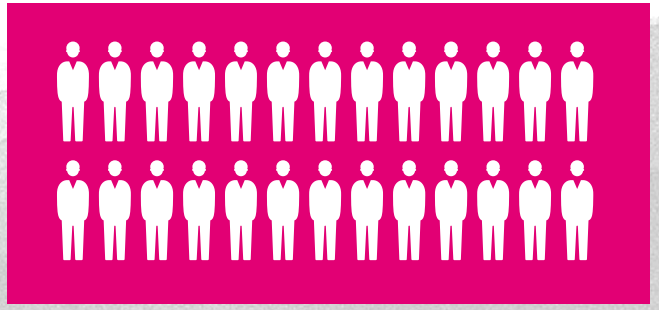
wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS



T · · Systems ·

INFRASTRUCTURE & APPLICATION SECURITY
WIR UNTERSTÜTZEN SIE

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS



60 Experten im Bereich Penetrationstest und IT – Forensik

- Berater,
- technische Sicherheitsexperten,
- Penetrationtester,
- Projektmanager,
- Auditoren,

anerkannte Zertifizierungen: z.B. als

- Certified Ethical Hacker (CEH)
- GIAC Certified Forensic Analyst (GCFA)
- GIAC Network Forensic Analyst (GNFA)
- GIAC Mobile Device Security Analyst
- Certified Security Analyst (ECSA)
- Web Application Penetration Tester (GWAPT)
- Oracle Certified Professional Java SE7 Programmer (OCPJP)
- SAP ADM960 SAP Netweaver AS - Security
- Certified Scada Security Architect (CSSA)
- ISTQB Certified Tester, Test Manager
- TeleTrusT Information Security Professional (T.I.S.P.)

T · · Systems ·

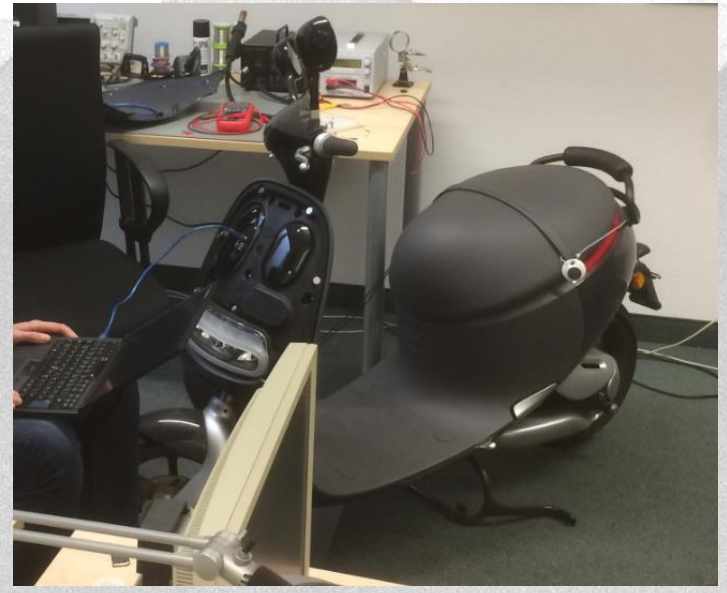
PENETRATIONSTEST UND FORENSIK

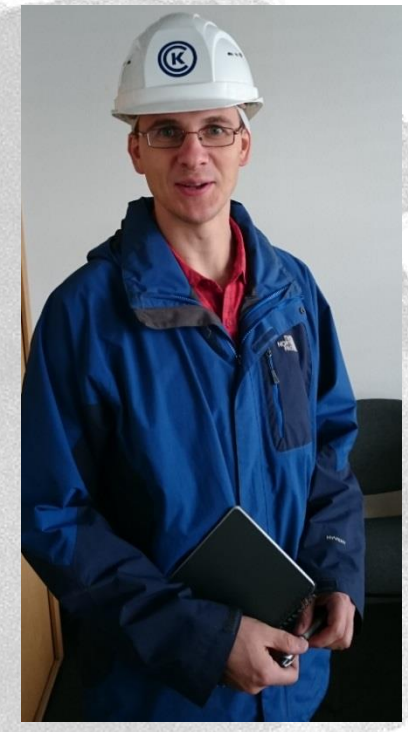
wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

T · · Systems ·

PENETRATIONSTEST UND FORENSIK

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 ·