MMS EXPERIENCE BEYOND DIGITAL

PENETRATIONSTEST

T-Systems Multimedia Solutions Certified Security

T · · Systems · Let's power higher performance

Motivation

Motivation

"Dark Souls": Spiele-Entwickler nimmt Server wegen Exploit vom Netz

Die PC-Server von Spielen der "Dark Souls"-Reihe sind derzeit offline. Hintergrund ist ein Exploit, der es Angreifern erlauben soll, Schadcode zu verteilen.

Virenscan-Dienste

Vertrauliche Nutzer-Dokumente öffentlich abrufbar

Arztberichte, Arbeitsverträge, Bewerbungen, Unfallgutachten – all das fanden wir auf Virenscan-Plattformen, arglos hochgeladen von Nutzern der Analysedienste.

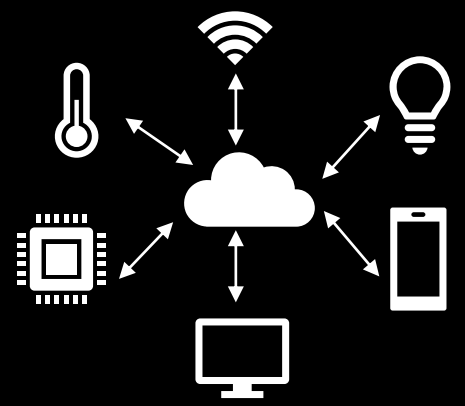
Sicherheitsupdates Atlassian Jira: Angreifer könnten Authentifizierung umgehen

Die Entwickler haben eine kritische Sicherheitslücke im Projektmanagement-Tool Jira geschlossen.

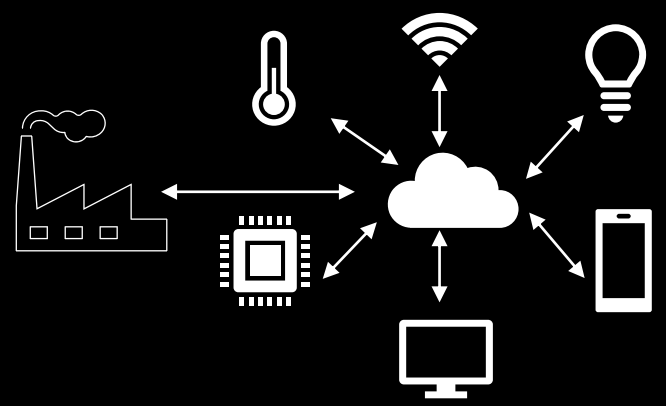
Datenleck im Legoland: Reisedaten tausender Kunden betroffen

Durch ein Datenleck der Buchungsseite für Legoland-Übernachtungen im bayerischen Günzburg waren Kundendaten der letzten sieben Jahre öffentlich einsehbar.

Zunehmende Vernetzung – Erhöhung der Komplexität



„intelligente“ Gegenstände mit „smarten“ Funktionen



Industrielle Ausprägung des IoT

Penetrationstest

Herausforderungen

- Aufspüren von Sicherheitslücken in infrastrukturen oder Anwendungen, bevor andere sie zu Ihrem Schaden ausnutzen können
- Bewertung des Sicherheitsniveaus
- Identifikation von Schwachstellen
- Erstellung eines detaillierten Maßnahmenkataloges mit Empfehlungen

MMS EXPERIENCE BEYOND DIGITAL

Hacking vs. Penetrationstest

T · · Systems · Let's power higher performance

Hacking

- Skills?
- Motivation?

Gesetzeslage

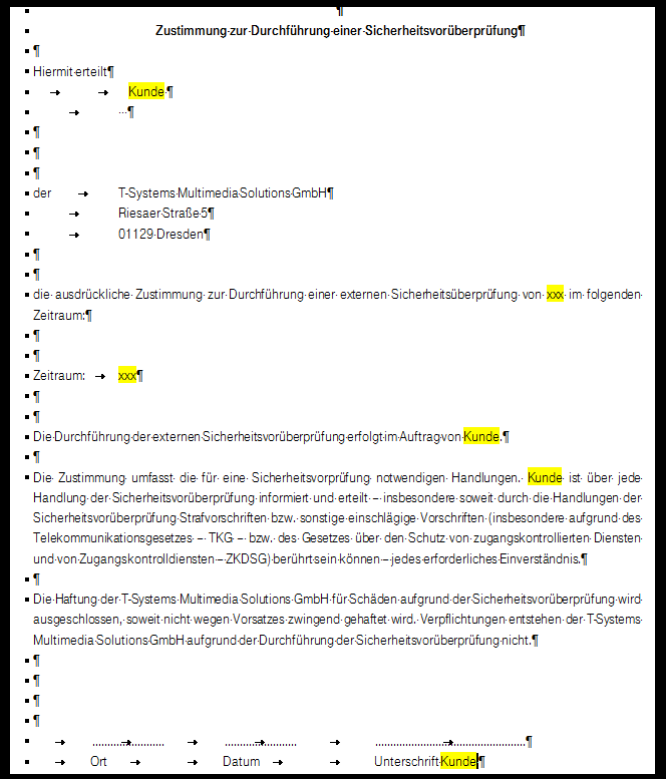
Hackerparagraph §202c "Vorbereiten des Ausspähens und Abfangens von Daten"

(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.

Penetrationstest



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 erforderliche 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

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

Scope definieren

Angreiferperspektive

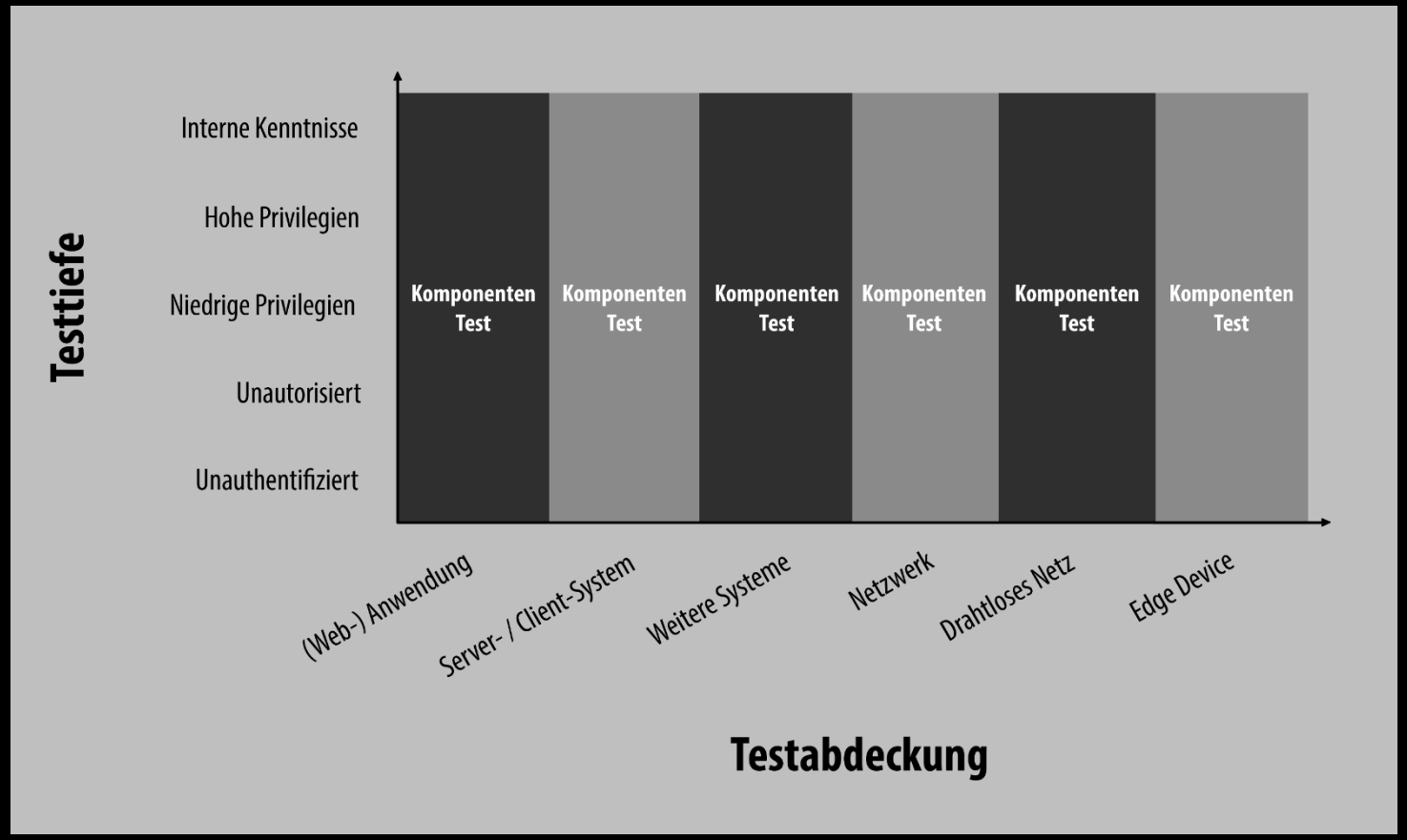
- Beschreibt mögliche Angreifer und deren Zugriffsmöglichkeiten, Privilegien, Voraussetzungen
- Gegen welche Art Angreifer soll das System geschützt werden?
  - Beispiele:
    - Externer, nicht privilegierter Angreifer (z.B. jemand mit Zugang zum Gerät aber ohne Zugriff auf Gerätefunktionen)
    - Externer, privilegierter Angreifer (z.B. Käufer, Endnutzer)
    - Interner, nicht privilegierter Angreifer (z.B. Gastzugang)
    - Interner, niedrig privilegierter Angreifer (z.B. Mitarbeiter)
    - Interner, hoch privilegierter Angreifer (z.B. Administrator)
- Eine oder mehrere Perspektiven müssen im Rahmen des Testplanung abgestimmt werden
- Aus diesen lassen sich Testabdeckung und Testtiefe ableiten

Testabdeckung

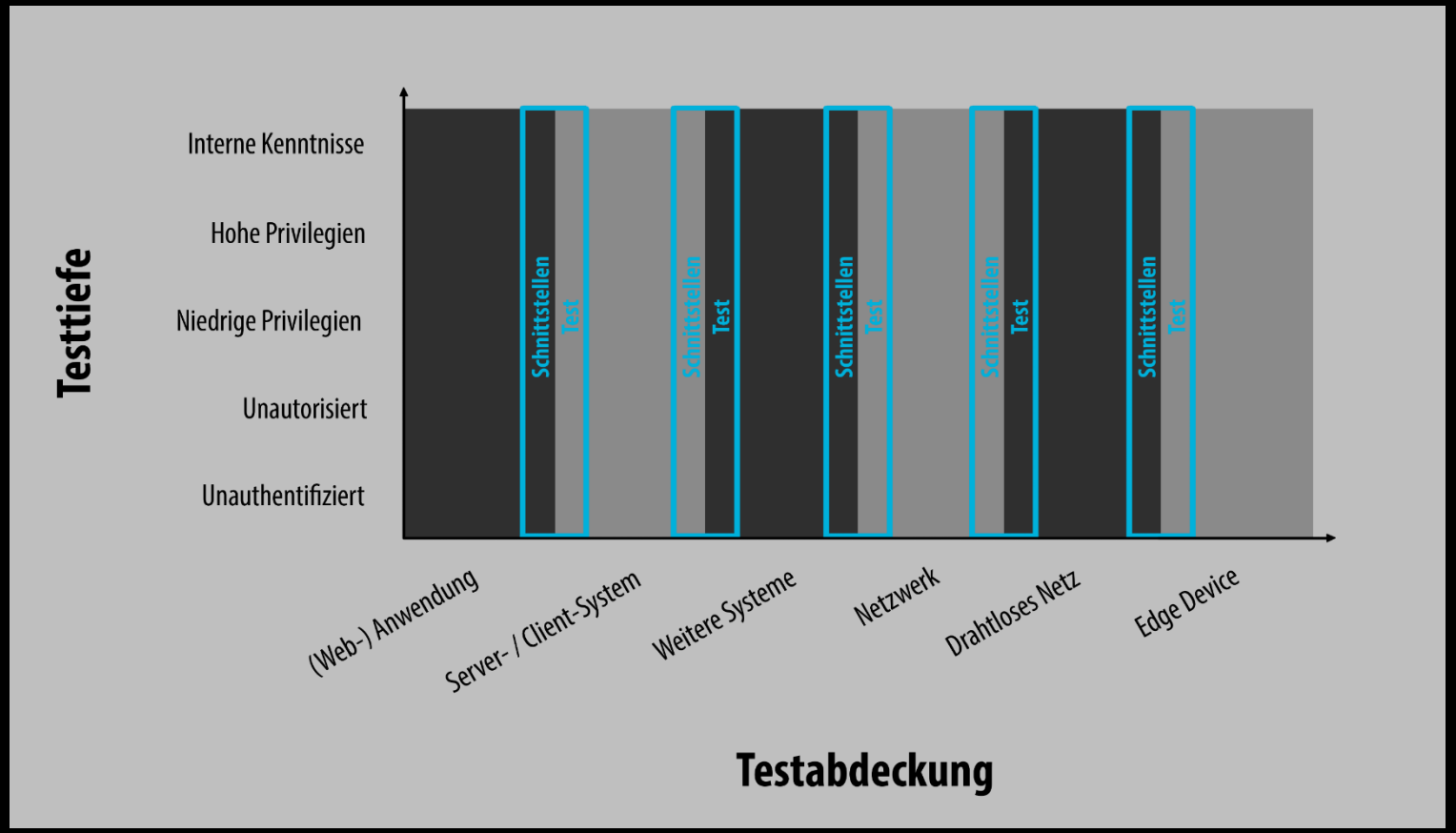
- Legt fest, wie viele und welche Komponenten getestet werden sollen
- Testobjekte, welche im Rahmen des Tests untersucht werden
- Beispiele:
  - Einzelne Komponenten (z.B. Webanwendungen, Server)
  - Einzelne Schnittstellen (z.B. APIs, Funkschnittstellen)
  - Ende-zu-Ende Test (vom Gerät über die API bis zur Webanwendung)

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

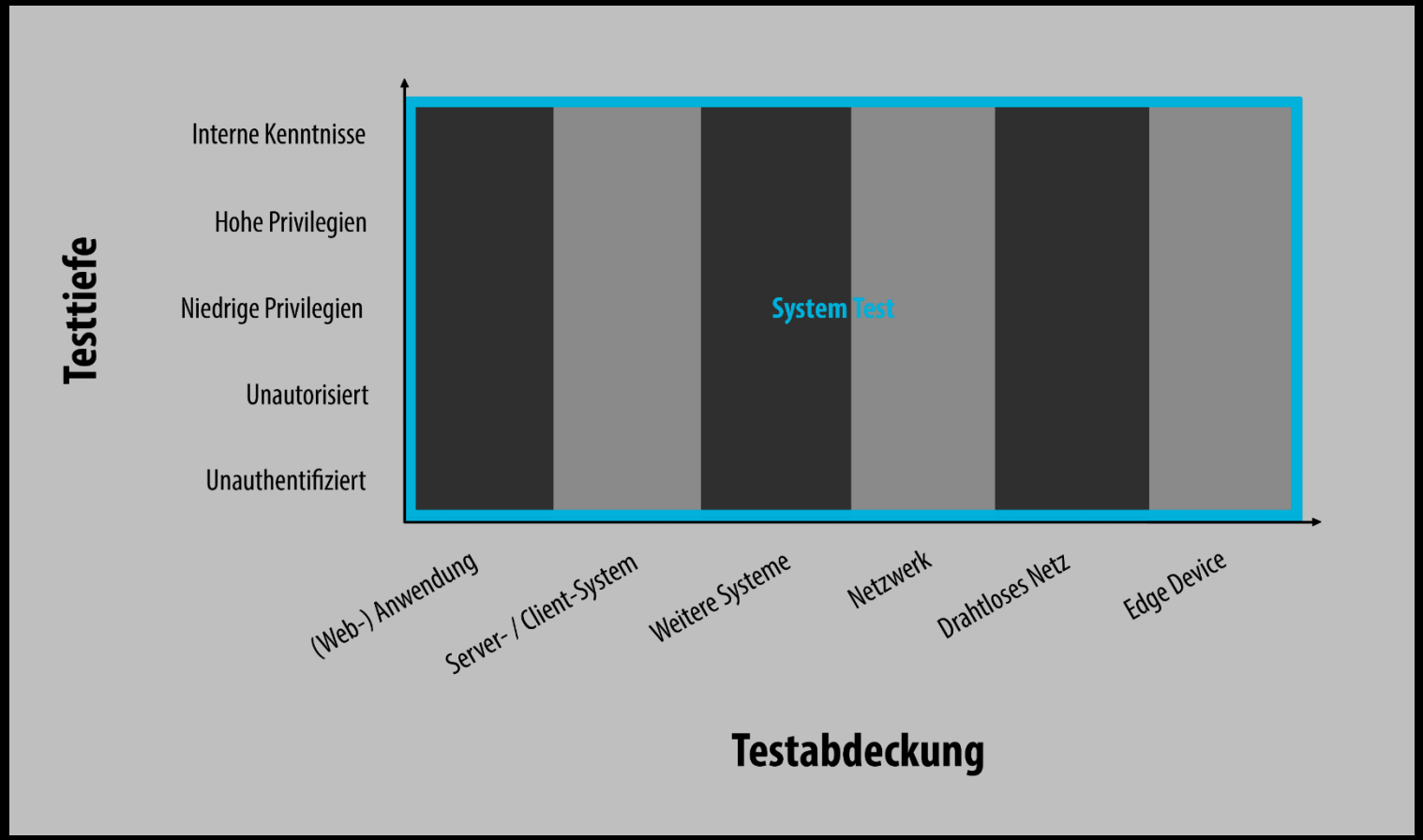
Testabdeckung



Testabdeckung



Testabdeckung



Testabdeckung

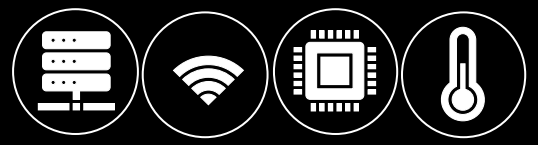
Delta-Tests

Vergleich zwischen zwei verschiedenen Systemversionen

Testabdeckung

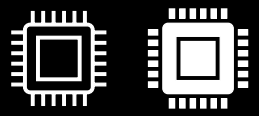
Vergleich

- 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

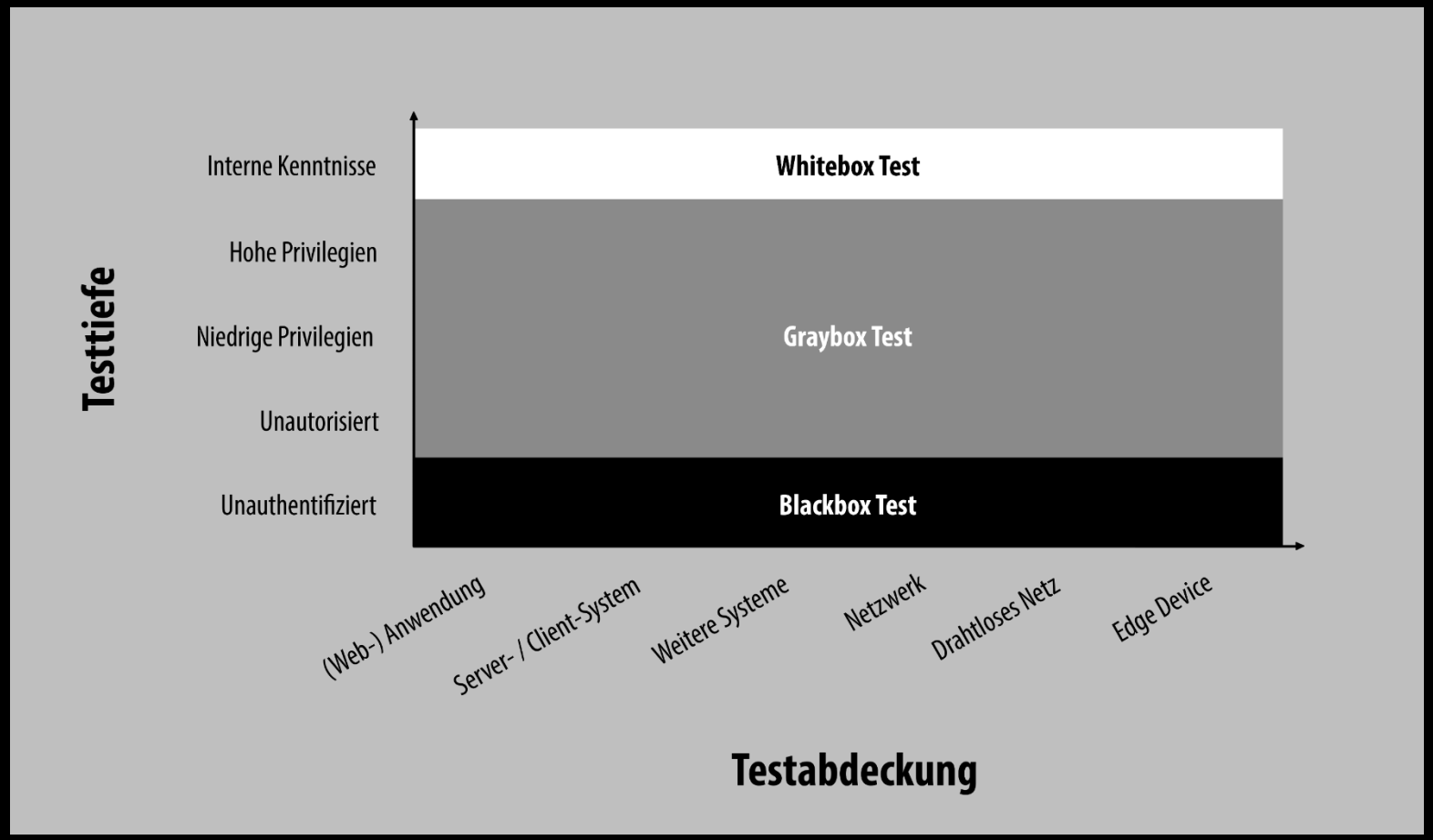


Delta-Tests

Testtiefe

- 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


Testtiefe
Interne Kenntnisse
Hohe Privilegien
Niedrige Privilegien
Unautorisiert
Unauthentifiziert
Whitebox Test
Graybox Test
Blackbox Test
(Web-) Anwendung
Server- / Client-System
Weitere Systeme
Netzwerk
Drahtloses Netz
Edge Device
Testabdeckung

Testtiefe

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

Testtiefe

Greybox

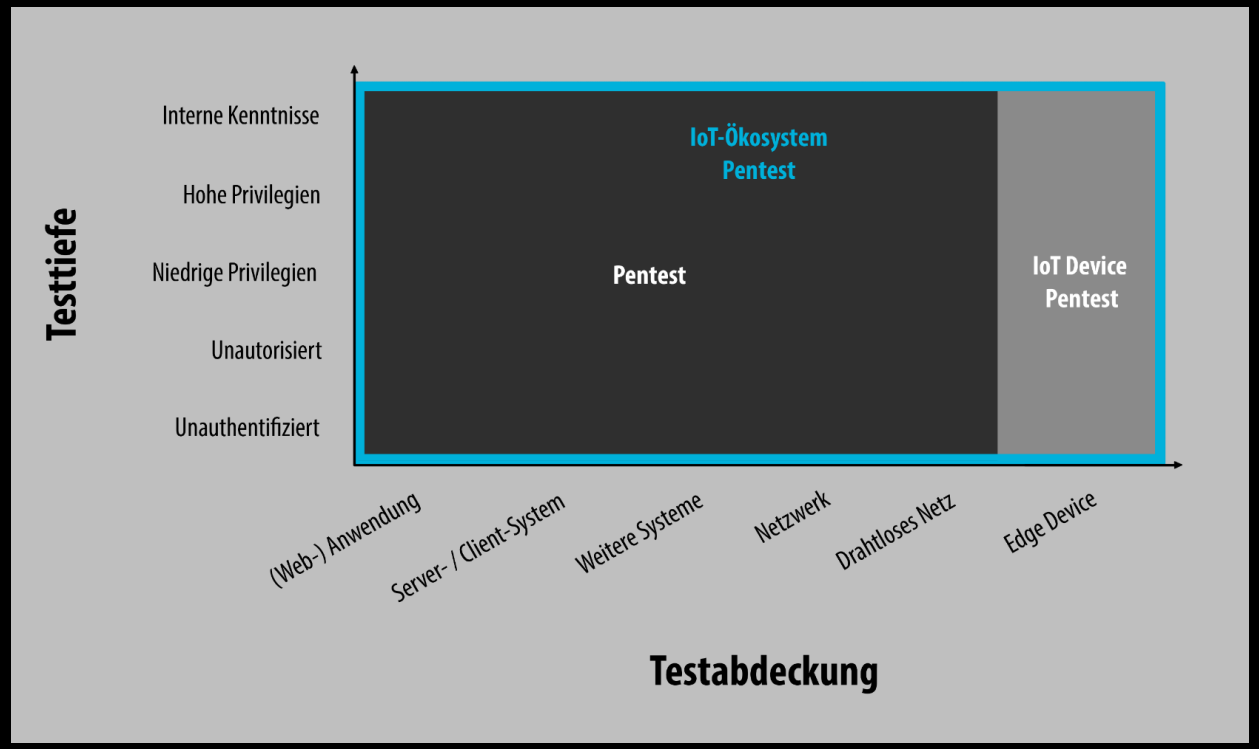
- Stellt eine Mischform aus Black- und Whitebox-Test dar
- Entsprechend geringere Kosten als bei Whitebox
- Nicht vollumfänglich wie Whitebox

Explorativ

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

Testschwerpunkte

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



Testart: Schwachstellen-Scan

M M S EXPERIENCE BEYOND DIGITAL

- 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.

Testart: Penetrationstest

M M S EXPERIENCE BEYOND DIGITAL

- 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.
- Prüfpunkte: systematisches Vorgehen im Test, standardisierte Testfälle
  - Web: z. B. https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/

Testart: Source Code Analyse

M M S EXPERIENCE BEYOND DIGITAL

- 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.

Das Angebot

- 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

Testvorgehen

Vorgehensmodell

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

Penetrationstest – Prozess –Phase 1

M M S EXPERIENCE BEYOND DIGITAL

Vorbereitung

- Ziele, Umfang und Vorgehen festlegen
- Testumgebung, Testvoraussetzungen definieren
- Rechtliche bzw. organisatorische Aspekte klären
- Risiken und erforderliche Notfallmaßnahmen abstimmen

Informations-beschaffung

- Übersicht über installierte Systeme und Anwendungen
- Recherche benötigter Informationen
- Bestimmung potenzieller Angriffspunkte bzw. bekannter Sicherheitsmängel

Bewertung

- Analyse und Bewertung der gesammelten Informationen
- Priorisierung und Auswahl der relevanten Testmodule
- Auswahl von Testfällen

Aktive Eindring-versuche

- Durchführung aktiver Angriffsversuche auf die ausgewählten Systeme
- Verifikation und Dokumentation der identifizierten Schwachstellen

Abschlussanalyse

- Erstellung der Abschluss-dokumentation
- Bewertung der Ergebnisse
- Darstellung der Risiken
- Definition von Maßnahmen

Penetrationstest – Prozess –Phase 2

M M S EXPERIENCE BEYOND DIGITAL

Vorbereitung

- Ziele, Umfang und Vorgehen festlegen
- Testumgebung, Testvoraussetzungen definieren
- Rechtliche bzw. organisatorische Aspekte klären
- Risiken und erforderliche Notfallmaßnahmen abstimmen

Informations-beschaffung

- Übersicht über installierte Systeme und Anwendungen
- Recherche benötigter Informationen
- Bestimmung potenzieller Angriffspunkte bzw. bekannter Sicherheitsmängel

Bewertung

- Analyse und Bewertung der gesammelten Informationen
- Priorisierung und Auswahl der relevanten Testmodule
- Auswahl von Testfällen

Aktive Eindring-versuche

- Durchführung aktiver Angriffsversuche auf die ausgewählten Systeme
- Verifikation und Dokumentation der identifizierten Schwachstellen

Abschlussanalyse

- Erstellung der Abschluss-dokumentation
- Bewertung der Ergebnisse
- Darstellung der Risiken
- Definition von Maßnahmen

Penetrationstest – Prozess –Phase 3

M M S EXPERIENCE BEYOND DIGITAL

Vorbereitung

- Ziele, Umfang und Vorgehen festlegen
- Testumgebung, Testvoraussetzungen definieren
- Rechtliche bzw. organisatorische Aspekte klären
- Risiken und erforderliche Notfallmaßnahmen abstimmen

Informationsbeschaffung

- Übersicht über installierte Systeme und Anwendungen
- Recherche benötigter Informationen
- Bestimmung potenzieller Angriffspunkte bzw. bekannter Sicherheitsmängel

Bewertung

- Analyse und Bewertung der gesammelten Informationen
- Priorisierung und Auswahl der relevanten Testmodule
- Auswahl von Testfällen

Aktive Eindringversuche

- Durchführung aktiver Angriffsversuche auf die ausgewählten Systeme
- Verifikation und Dokumentation der identifizierten Schwachstellen

Abschlussanalyse

- Erstellung der Abschlussdokumentation
- Bewertung der Ergebnisse
- Darstellung der Risiken
- Definition von Maßnahmen

Penetrationstest – Prozess –Phase 4

M M S EXPERIENCE BEYOND DIGITAL

Vorbereitung

- Ziele, Umfang und Vorgehen festlegen
- Testumgebung, Testvoraussetzungen definieren
- Rechtliche bzw. organisatorische Aspekte klären
- Risiken und erforderliche Notfallmaßnahmen abstimmen

Informationsbeschaffung

- Übersicht über installierte Systeme und Anwendungen
- Recherche benötigter Informationen
- Bestimmung potenzieller Angriffspunkte bzw. bekannter Sicherheitsmängel

Bewertung

- Analyse und Bewertung der gesammelten Informationen
- Priorisierung und Auswahl der relevanten Testmodule
- Auswahl von Testfällen

Aktive Eindringversuche

- Durchführung aktiver Angriffsversuche auf die ausgewählten Systeme
- Verifikation und Dokumentation der identifizierten Schwachstellen

Abschlussanalyse

- Erstellung der Abschlussdokumentation
- Bewertung der Ergebnisse
- Darstellung der Risiken
- Definition von Maßnahmen

Penetrationstest – Prozess –Phase 5

M M S EXPERIENCE BEYOND DIGITAL

Vorbereitung

- Ziele, Umfang und Vorgehen festlegen
- Testumgebung, Testvoraussetzungen definieren
- Rechtliche bzw. organisatorische Aspekte klären
- Risiken und erforderliche Notfallmaßnahmen abstimmen

Informationsbeschaffung

- Übersicht über installierte Systeme und Anwendungen
- Recherche benötigter Informationen
- Bestimmung potenzieller Angriffspunkte bzw. bekannter Sicherheitsmängel

Bewertung

- Analyse und Bewertung der gesammelten Informationen
- Priorisierung und Auswahl der relevanten Testmodule
- Auswahl von Testfällen

Aktive Eindringversuche

- Durchführung aktiver Angriffsversuche auf die ausgewählten Systeme
- Verifikation und Dokumentation der identifizierten Schwachstellen

Abschlussanalyse

- Erstellung der Abschlussdokumentation
- Bewertung der Ergebnisse
- Darstellung der Risiken
- Definition von Maßnahmen

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

M M S EXPERIENCE BEYOND DIGITAL

Bewertung: nach CVSS 3.1 (Base Score): https://www.first.org/cvss/calculator/3.1

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)

Testbericht Penetrationstest

M M S EXPERIENCE BEYOND DIGITAL

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

MMS EXPERIENCE BEYOND DIGITAL

Certified Security @ TSI MMS

T · · Systems · Let's power higher performance

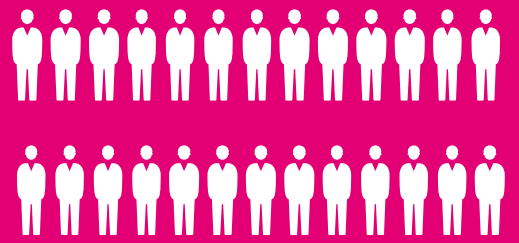
Certified Quality

M M S EXPERIENCE BEYOND DIGITAL

Die Business Unit Certified Quality & Intelligent Automation sorgt mit Ihrem Test und Integration Center (einem von der DAkkS nach DIN EN ISO/IEC 17025 akkreditierten Software-Prüflabor der Multimedia-Branche) und als BSI zertifizierter IT-Sicherheitsdienstleister mit 250 Quality-Engineers und Security-Spezialisten für die digitale Zuverlässigkeit von Software, digitalen Anwendungen und Geschäftsprozessen ihrer Kunden: innovativ, automatisiert, nutzerzentriert und sicher.

DAkkS
Deutsche Akkreditierungsstelle
D-PL-12109-01-00

Certified Security



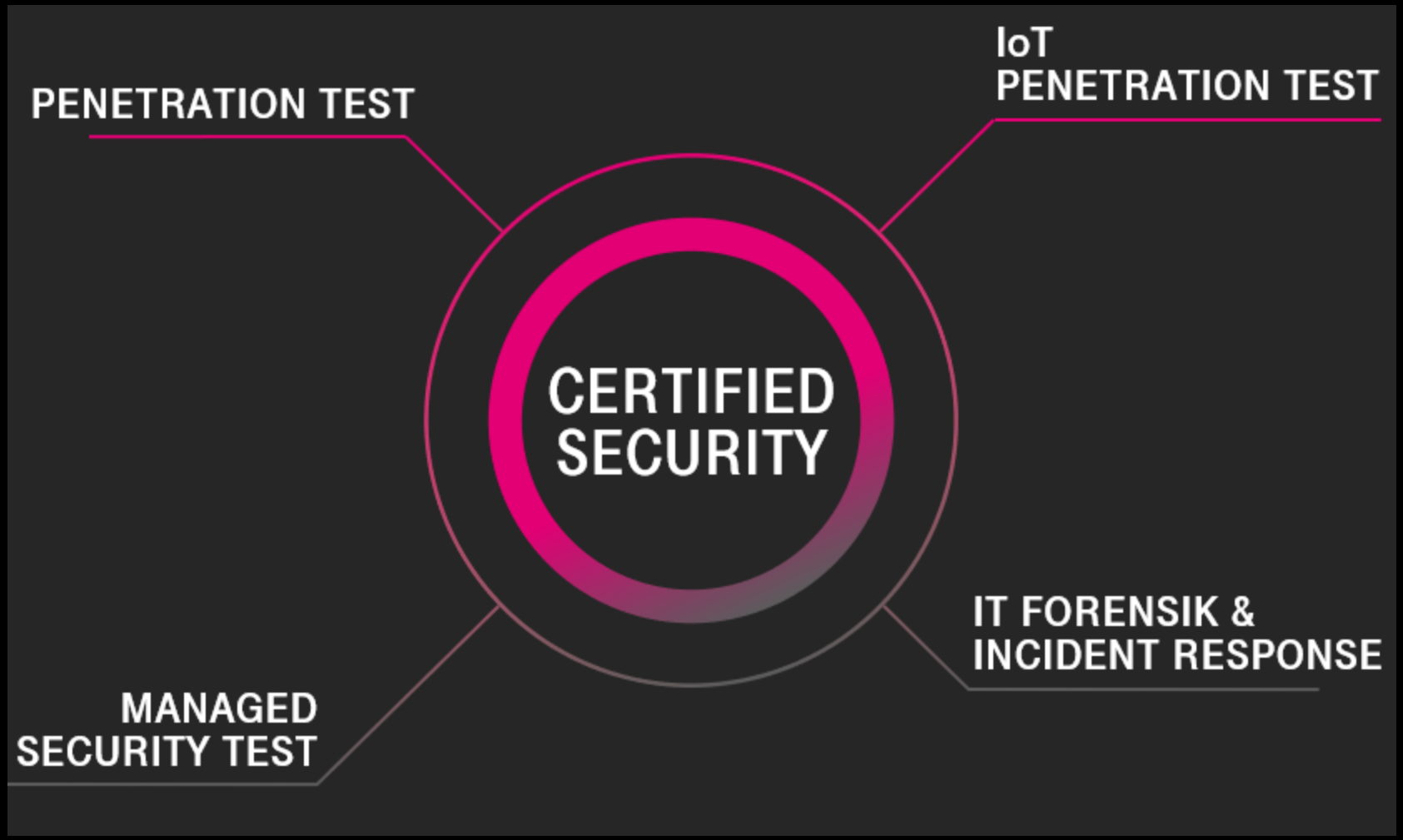
Zertifiziertes Testlabor + 60 Experten im Bereich Penetrationstest und IT – Forensik

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

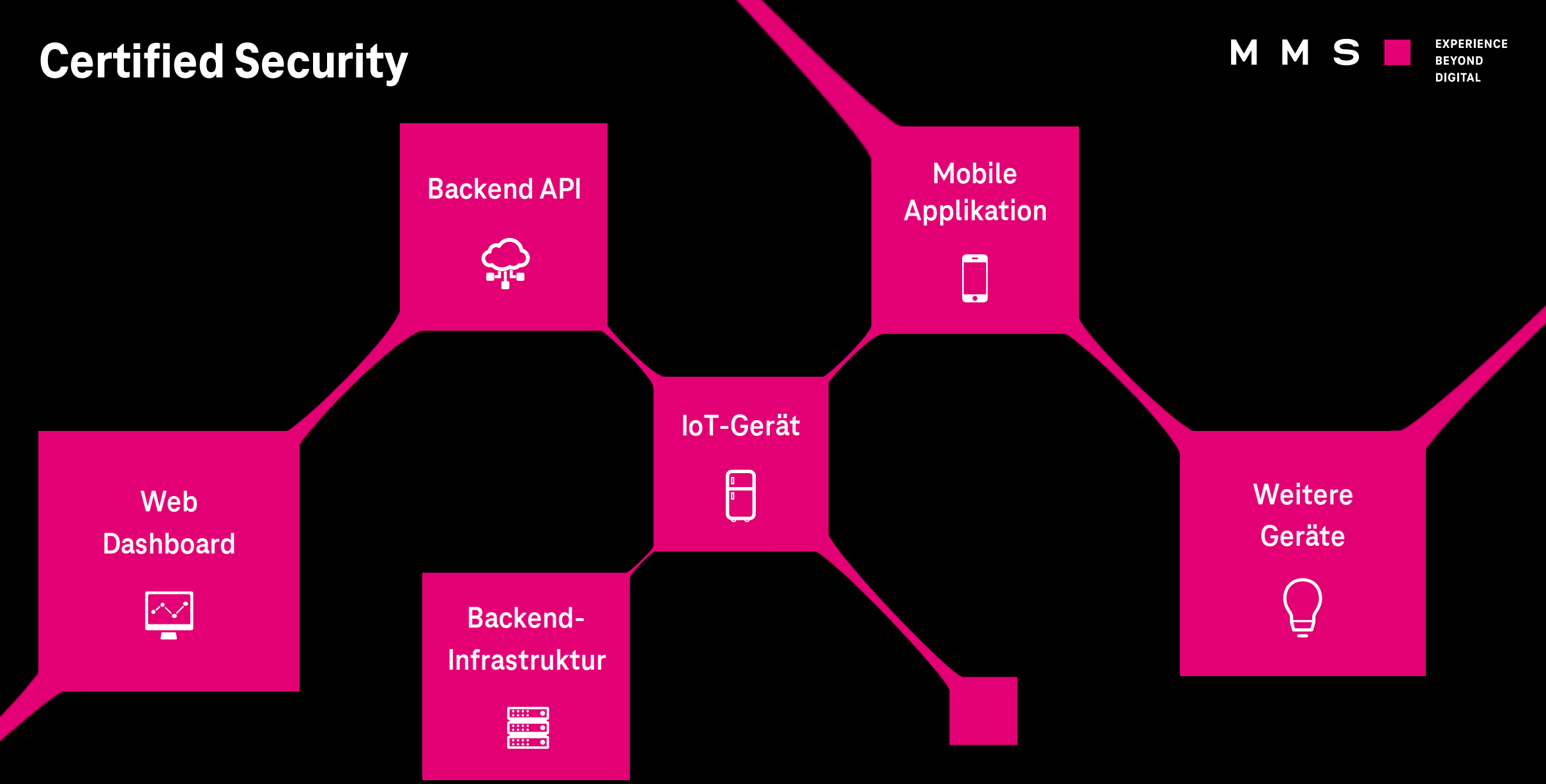
Anerkannte Zertifizierungen:

- ISTQB Certified Tester, Test Manager
- Certified Ethical Hacker (CEH)
- BSI Common Criteria 3.1 Evaluator
- Offensive Security Certified Professional (OSCP)
- Offensive Security Certified Expert (OSCE)
- Advanced Web Attacks and Exploitation (AWAE)
- GIAC Reverse Engineering Malware (GREM)
- GIAC Advanced Smartphone Forensic (GASF)
- GIAC Mobile Device Security Analyst
- Certified Security Analyst (ECSA)
- Web Application Penetration Tester (GWAPT)
- Certified Information Systems Security Professional (CISSP)
- TeleTrusT Information Security Professional (T.I.S.P.)

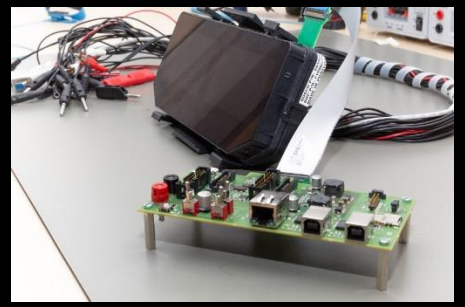
Certified Security

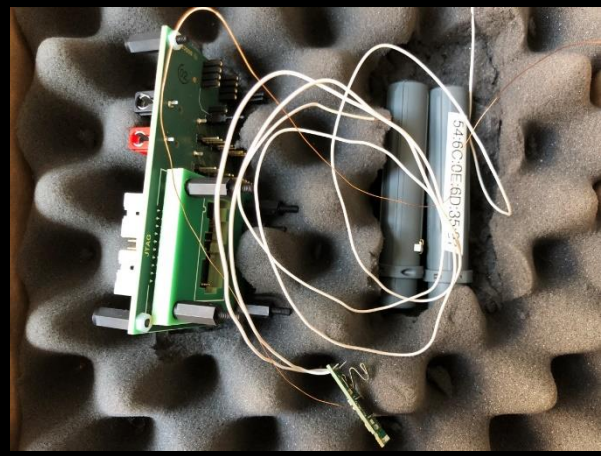


Certified Security



Certified Security





Nützliche Links

Ausbildung

- eLearnSecurity - Junior Penetration Tester (eJPT): https://elearnsecurity.com/product/ejpt-certification/

Hacking Labs

- HackTheBox: https://www.hackthebox.eu/
- OWASP Juice Shop: https://github.com/bkimminich/juice-shop
- PortSwigger Academy https://portswigger.net/web-security

Konferenzen

- DEFCON: https://media.defcon.org/
- OffensiceCon: https://www.offensivecon.org
- Blackhat: https://www.blackhat.com/

MMS EXPERIENCE BEYOND DIGITAL

Kontakt

Dr. Antje Winkler
Telefon: +49 351 2820 2093
Mail: Antje.Winkler@t-systems.com

T · · Systems · Let's power higher performance